NEGER Telecom

NEGER VPN Pro
3G Router

Advanced
User Guide

Copyright

Trademarks

All products, company, brand names are trademarks or registered trademarks of their respective companies. They are used for identification purpose only. Specifications are subject to be changed without prior notice.

FCC Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against radio interference in a commercial environment. This equipment can generate, use and radiate radio frequency energy and, if not installed and used in accordance with the instructions in this manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause interference, in which case the user, at his own expense, will be required to take whatever measures are necessary to correct the interference.

CE Declaration of Conformity

This equipment complies with the requirements relating to electromagnetic compatibility, EN 55022/A1 Class B.

The specification is subject to change without notice.

Table of Contents

1. Introduction

The NEGER VPN Pro 3G Router is a high-performance tool that supports wireless networking at home, work, or in a public place. The NEGER VPN Pro 3G Router supports uses a USB 3G modem card, either WCDMA or EVDO and even HSDPA as well, and supports wireless data transfers up to 30Mbps, and wired data transfers up to 100 Mbps.
The NEGER VPN Pro 3G Router is compatible with industry security features.

1.1. Package Contents

Importance: Check your product package contents FIRST.

The NEGER VPN Pro 3G Router package should contain the items listed below. If any of the items are missing, please contact your reseller.

items	Description	Quantity
1	NEGER VPN Pro 3G Router	1
2	RJ-45 Cable	1
3	Power adapter 12V / 2.0A	1
4	User Manual	1
5	External WiFi Antenna	1

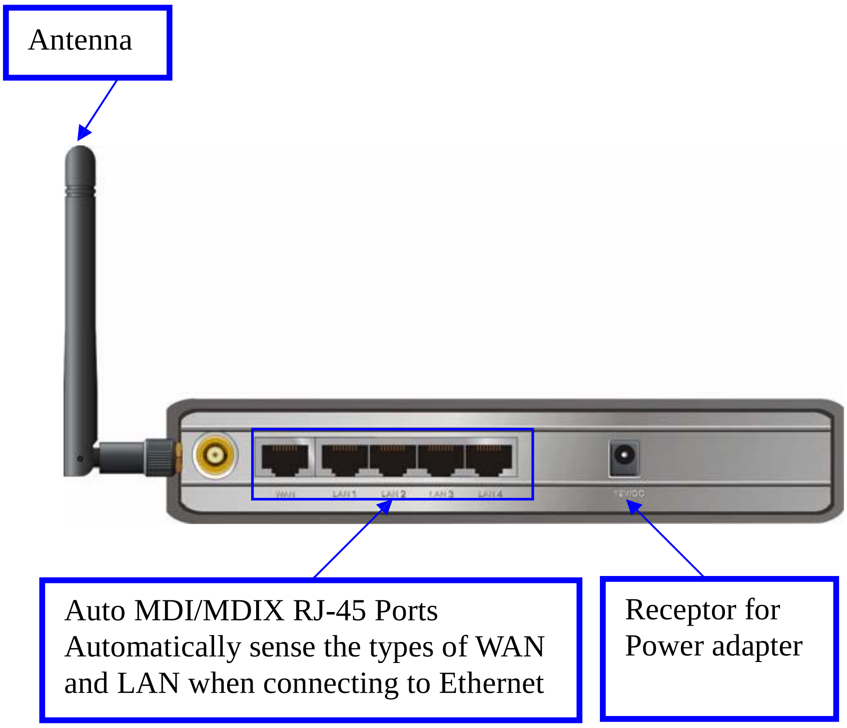
Caution: Using a power supply with a different voltage rating than the one included with the NEGER VPN Pro 3G Router will cause damage and void the warranty for this product.

1.2. System Requirements for Configuration

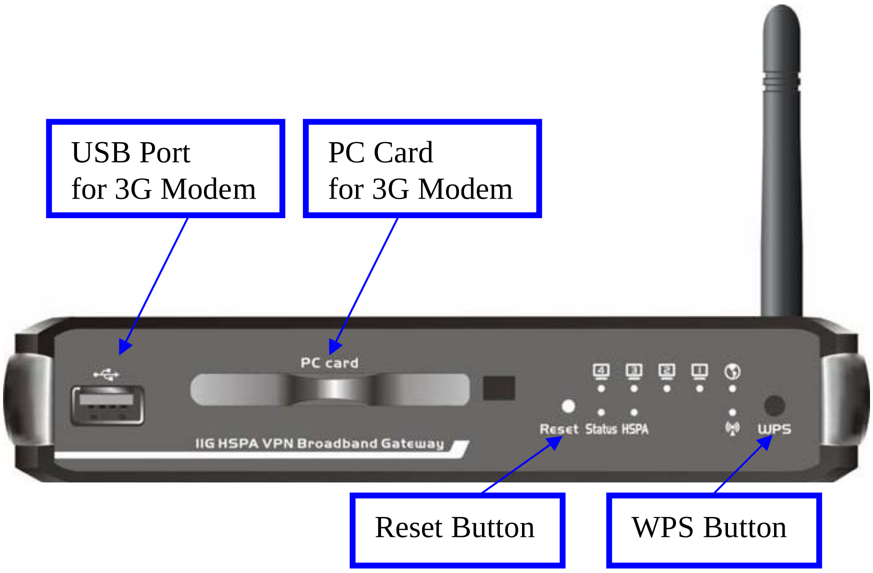
• A 3G SIM Card *with service*
Note: Subject to services and service terms available from your carrier.
• Computers with Windows, Macintosh, or Linux-based operating systems with an installed Ethernet adapter.
• Internet Explorer version 6.0 or Netscape Navigator version 7.0 and above.
• Wi-Fi System Requirements: An 802.11b, 802.11g, or 802.11n Adapter.

1.3. Interfaces

The Rear View

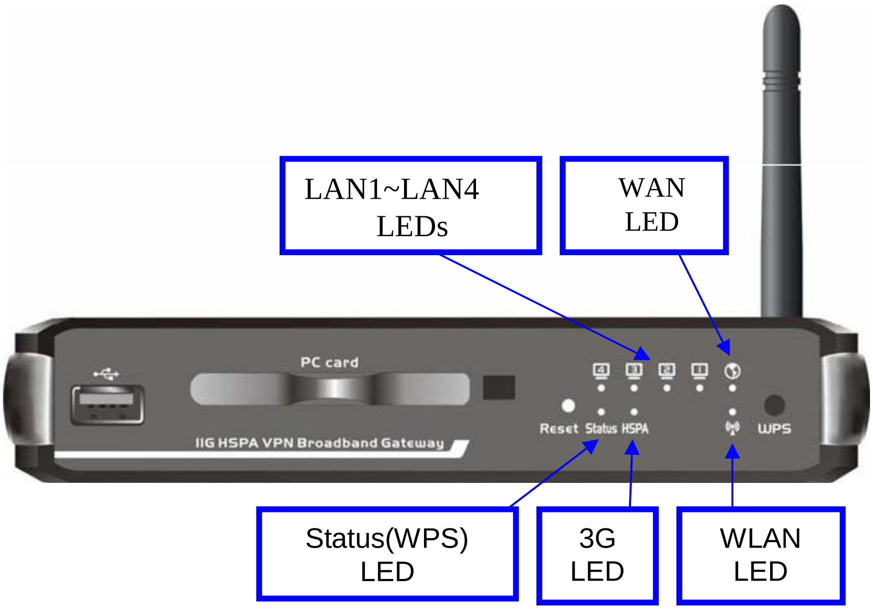

Antenna
WAN
LAN 1
LAN 2
LAN 3
LAN 4
12V/DC
Auto MDI/MDIX RJ-45 Ports
Automatically sense the types of WAN and LAN when connecting to Ethernet
Receptor for Power adapter

The Front View



Note:
Contains a reset button to restore the setting back to original factory defaulted setting as if your convenience of forgetting your applicable setting

1.4. LEDs– the Front View



A. Status (WPS) LED :
   Green in flash: device status is normal
   Green in fast flash: device is in WPS PBC mode (The LED blinks 3 times per second, approximately 280~340ms.)

B. WAN LED:
   Green: Ethernet connection is established
   Green in flash: data packet transferred via Ethernet

C. LAN1 ~ LAN4 LEDs:
   Green: Ethernet connection is established
   Green in flash: data packet transferred via Ethernet

D. WLAN LED:
   Green: WLAN is active and available
   Green in flash: data packet transferred via WLAN

E. 3G LED:
   Green: 3G connection is established
   Green in flash: data packet transferred via 2G/2.5G

1.5. Features

- IEEE 802.11b/g compliant
  - Backward compatible to IEEE 802.11b standards
  - Max physical rate up to 54Mbps in 802.11g mode
  - Security Supports: WEP (64/128 bits), WPA, WPA2, WPA-PSK, WPA2-PSK, and 802.1x
  - WPS Support
- Provide 2 I/Fs for mobile HSPA network access
  - 1 * USB 2.0 port
  - 1 * Type II PC Card slot
- Provide 5 * 10/100 RJ-45 ports
  - 4 * LAN
  - 1 * WAN (Backup of 3G connection)
- WAN connection through Ethernet
  - Dynamic IP (DHCP Client)
  - Static IP
  - PPPoE
  - PPTP
  - L2TP
- PPTP over 3G WAN connection
- Built-in NAT function: one IP sharing with PCs
- Built-in firewall to protect your Intranet
- VPN support
  - Initiator and responder of IPSec, PPTP, and L2TP
  - Pass through of IPSec, PPTP, and L2TP
- Easy to upgrade firmware
  - Web UI
  - Windows utility
  - Quick Recover
- Easy to manage:
  - Web UI
  - SNMP
  - UPnP
- L3/L4 QoS
- Network Protocols
  - UDP/TCP/IP/ARP/RARP/ICMP
  - DHCP/PPPoE
  - DNS/TFTP/HTTP
- Connects multiple computers to a Broadband either WCDMA or EV-DO even HSDPA modem to share the Internet connection.

2. Configuring NEGER VPN Pro 3G Router

2.1. Installation Considerations

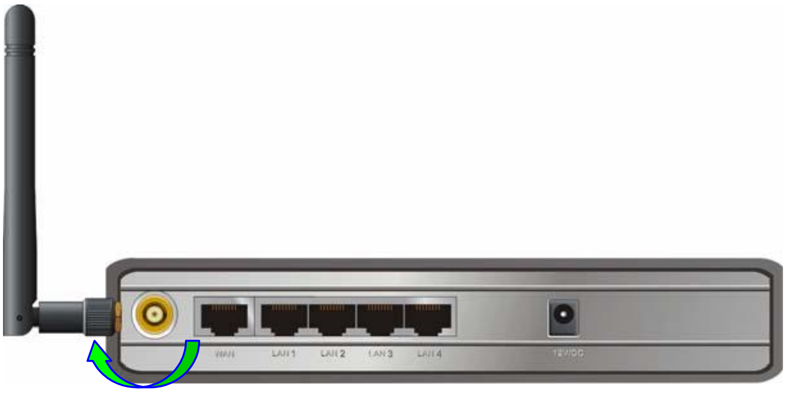
The NEGER VPN Pro 3G Router allows you access your network using a wireless connection, from virtually anywhere within its operating range. Keep in mind however, that the number, thickness, and location of walls, ceilings, or other objects that the wireless signals must pass through, may limit this range.
Typical ranges vary depending on the types of materials used, and background RF (radio frequency) noise in your home or business.

To maximize your wireless range, please follow these guidelines:

1. Keep the number of walls and ceilings between the NEGER VPN Pro 3G Router and other network devices to a minimum. Each wall or ceiling can reduce the NEGER VPN Pro 3G Router's range from 3-90 feet (1-30 meters).
   Note: The same considerations apply to your broadband EVDO connection.
2. Keep your product aware from electrical devices (such as microwaves, air conditioners, and televisions) that emit large quantities of RFI (Radio Frequency Interference).

2.1.1. Installation Instructions- Get Start Networking

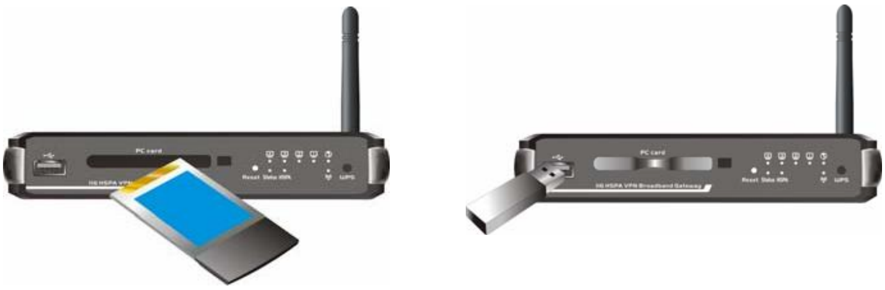
Connect the Wireless Router to Your Network
Note: *DO NOT connect NEGER VPN Pro 3G Router to power before performing the installation steps below.*
1. Attach the antenna. ---picture 2.1



Picture 2.1

a. Remove the antenna from its plastic wrapper.
b. Screw the antenna in a clockwise direction to the back panel of the unit.
c. Once secured, position the antenna upward at its connecting joint. This will ensure optimal reception.

2. Plug 3G Modem, either USB or PC Card to the Gateway **-- see Picture 2.2**



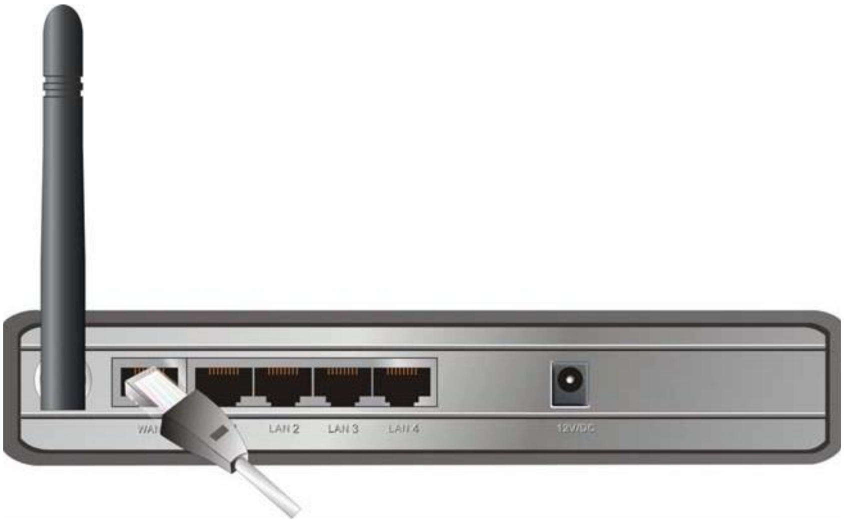
PC CARD

USB

Picture 2.2

Note: The **NEGER VPN Pro 3G Router** is designed to work with either UMTS or EV-DO and even HSUPA 3G modem. Please refer to your service provider for detailed feature information. (Reference the session 2: Using the Easy Setup Utility)

3. **(Option)** Insert the Ethernet patch cable into Wired WAN port on the back panel of the **NEGER VPN Pro 3G Router**. The step is option if you have inserted 3G modem. **-- see Picture 2.3**



Picture 2.3 (option)

Note: The **NEGER VPN Pro 3G Router** Wired WAN Port is "Auto-MDI/MDIX." This provides patch Ethernet cable Wired WAN Port access.

4. Insert the Ethernet patch cable into LAN Port on the back panel of the **NEGER VPN Pro 3G Router**, and an available Ethernet port on the network adapter in the computer you will use to configure the unit.**-see Picture 2.4**

WAN
LAN 1
LAN 2
LAN 3
LAN 4
12V/DC

Picture 2.4

Note: The Wireless WAN Mobile Broadband Router LAN Port is "Auto-MDI/MDIX." This provides patch Ethernet cable LAN Port access.

5. Connect the power adapter to the receptor on the back panel of your Wireless WAN Mobile Broadband Router. Then plug the other end of the power adapter into a wall outlet or power strip. ---Picture 2.5

WAN
LAN 1
LAN 2
LAN 3
LAN 4
12V/DC

Picture 2.5

6. The LEDs (See Picture 2.6)
   a. The LEDs will turn ON to indicate power has been applied.
   b. The Status LED will flash ON and OFF as the **NEGER VPN Pro 3G Router** performs initialization and Internet connection processes. This will take a few minutes.

Picture 2.6

2.1.2. Establish WiFi Connection

If you selected either **WEP** or **WPA-PSK** encryption, ensure these settings match your WiFi adapter settings.

WiFi and encryption settings must match for access to the **NEGER VPN Pro 3G Router** Configuration Menu, and the Internet. Please refer to your WiFi adapter documentation for additional information.

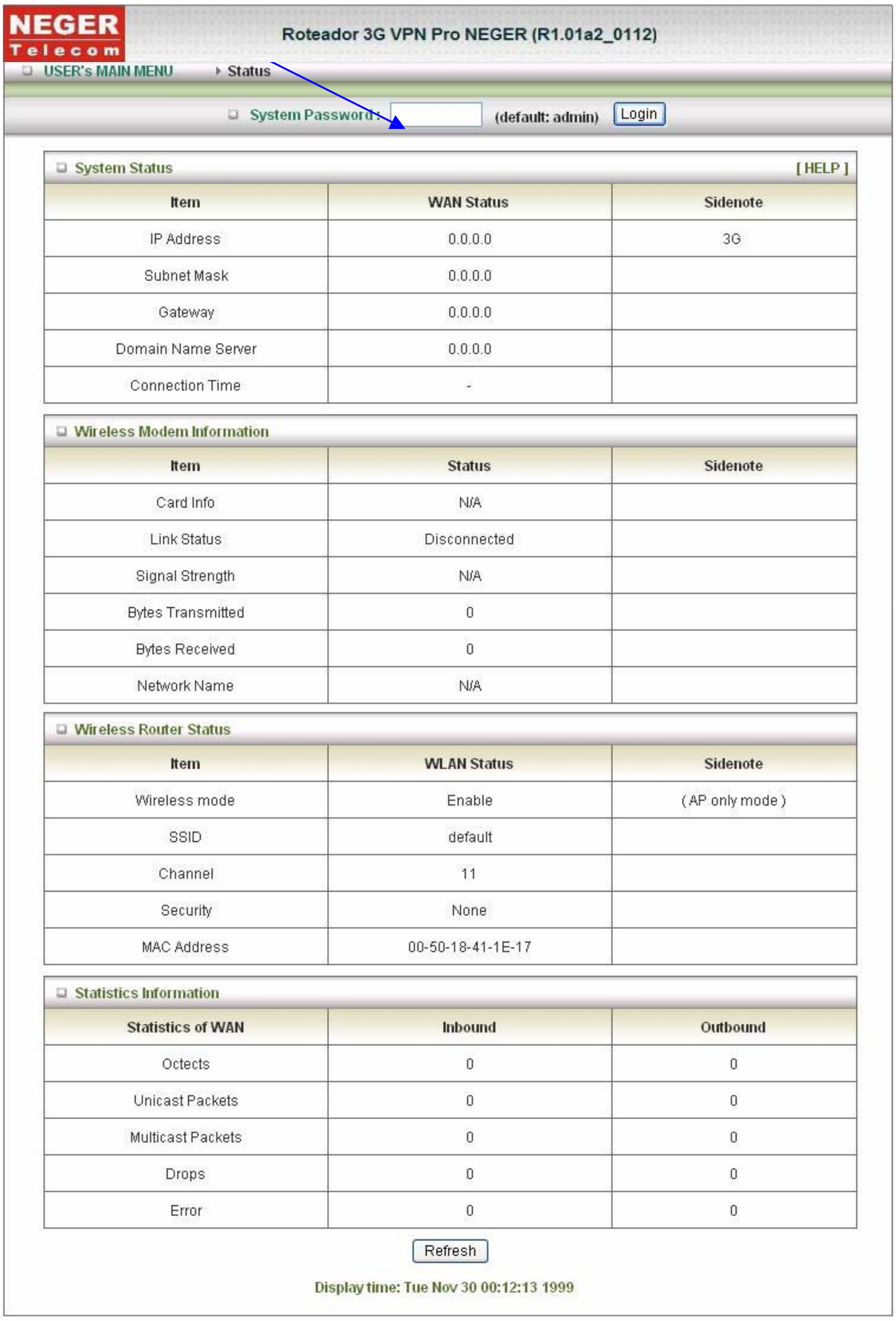
3. Using the Configuration Menu

Once properly configured, the **NEGER VPN Pro 3G Router** will obtain and assign IP address information automatically. Configuration settings can be established through the **NEGER VPN Pro 3G Router** Configuration Menu. You can access this interface by performing the steps listed below:

1. Open a web-browser.
2. Type in the **IP Address** (http://192.168.123.254) of the **NEGER VPN Pro 3G Router.**

Note: If you have changed the **default** IP Address assigned to the **NEGER VPN Pro 3G Router**, ensure you enter the correct IP Address now.

3. Type "**admin"** in the **Password**



System Status

Item	WAN Status	Sidenote
IP Address	0.0.0.0	3G
Subnet Mask	0.0.0.0	
Gateway	0.0.0.0	
Domain Name Server	0.0.0.0	
Connection Time	-	

Wireless Modem Information

Item	Status	Sidenote
Card Info	N/A	
Link Status	Disconnected	
Signal Strength	N/A	
Bytes Transmitted	0	
Bytes Received	0	
Network Name	N/A	

Wireless Router Status

Item	WLAN Status	Sidenote
Wireless mode	Enable	(AP only mode)
SSID	default	
Channel	11	
Security	None	
MAC Address	00-50-18-41-1E-17	

Statistics Information

Statistics of WAN	Inbound	Outbound
Octects	0	0
Unicast Packets	0	0
Multicast Packets	0	0
Drops	0	0
Error	0	0

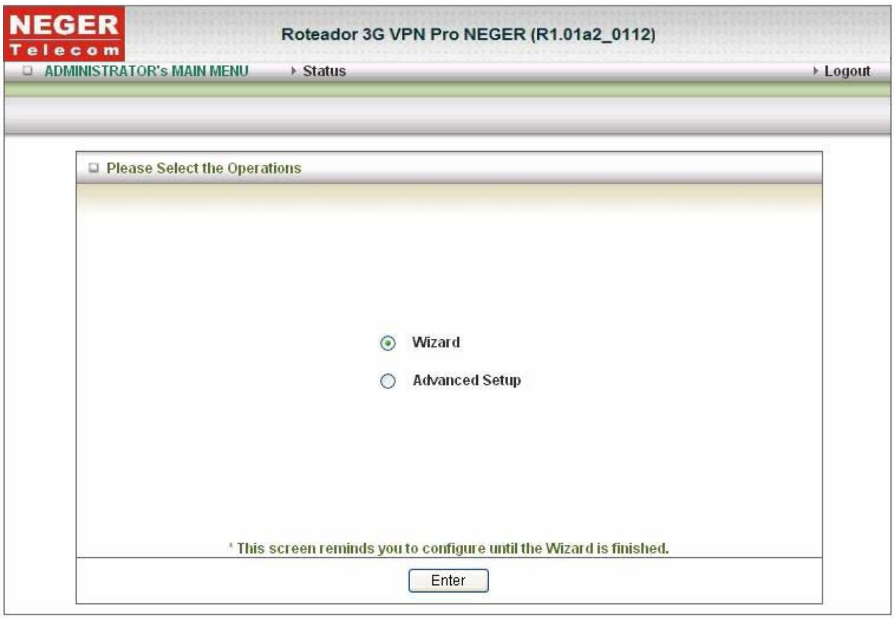
Display time: Tue Nov 30 00:12:13 1999

4. Click “logon” button.

3.1. Wizard setting

⌘ Press “**Wizard**” button for basic settings with simpler way. (Please check section 3.1)

⌘ Or you may click on “**Advanced Setup**” for advanced settings. (Please check the section Administrator’s Main Menu. each item from section 3.2)



Roteador 3G VPN Pro NEGER (R1.01a2_0112)

Please Select the Operations

● Wizard

○ Advanced Setup

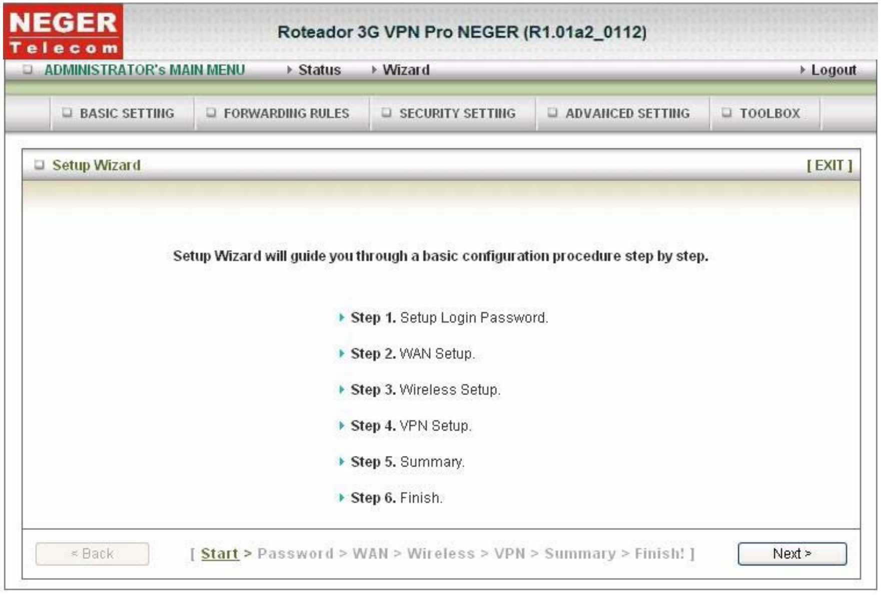
* This screen reminds you to configure until the Wizard is finished.

⌘ **Click on "Enter" button to get start.**

With wizard setting steps, you could configure the router in a very simple way. This configuration wizard includes settings of

a. **Login Password**,
b. **WAN Setup**,
c. **Wireless Setup**,
d. **VPN Setup**

Press **"Next"** button to start configuration.



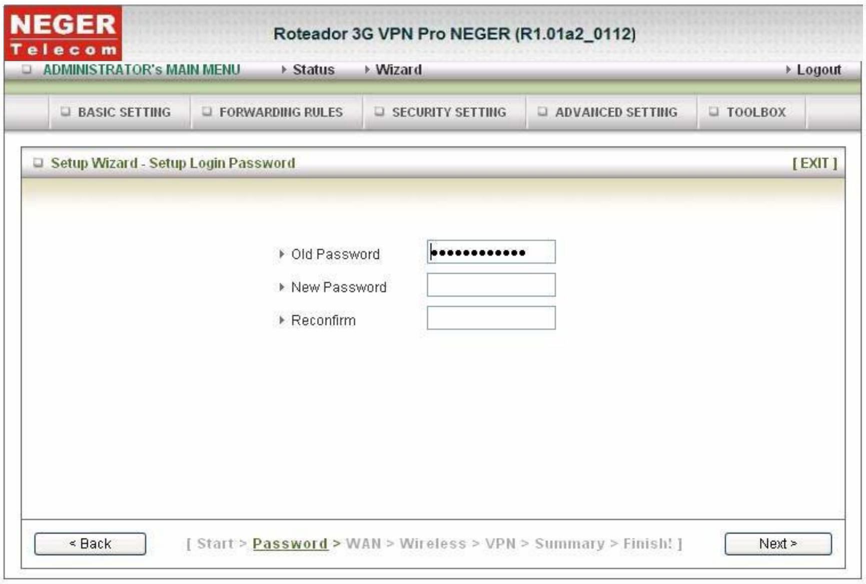
Roteador 3G VPN Pro NEGER (R1.01a2_0112)

Setup Wizard will guide you through a basic configuration procedure step by step.

- **Step 1.** Setup Login Password.
- **Step 2.** WAN Setup.
- **Step 3.** Wireless Setup.
- **Step 4.** VPN Setup.
- **Step 5.** Summary.
- **Step 6.** Finish.

< Back
[Start > Password > WAN > Wireless > VPN > Summary > Finish!]
Next >

Step 1: Allow you to change the system password.


NEGER Telecom
Roteador 3G VPN Pro NEGER (R1.01a2_0112)
ADMINISTRATOR's MAIN MENU
Status
Wizard
Logout
BASIC SETTING
FORWARDING RULES
SECURITY SETTING
ADVANCED SETTING
TOOLBOX
[EXIT]
< Back
[Start > Password > WAN > Wireless > VPN > Summary > Finish!]
Next >

Setup Wizard - Setup Login Password

Old Password •••••••••••••

New Password

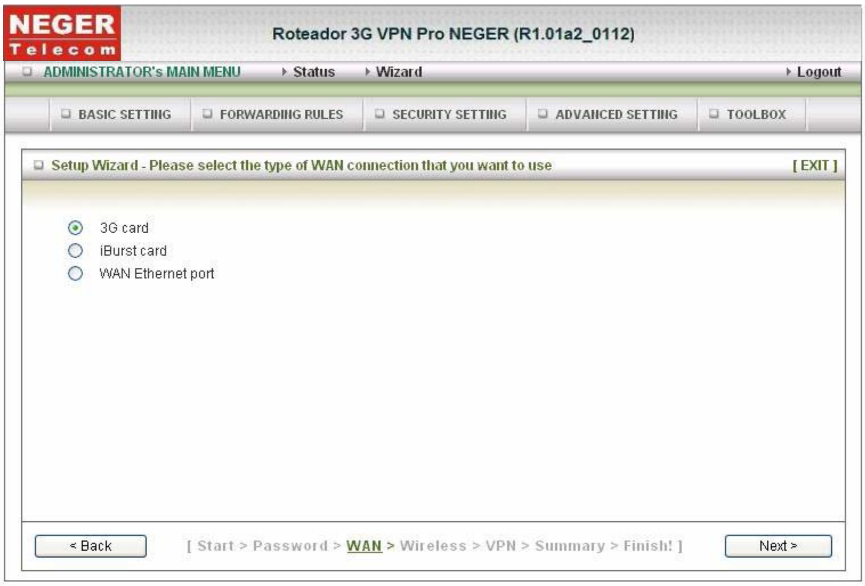
Reconfirm

You can change Password here.

It is recommended that you change the system password into the one you prefer to on the basis of security.

1. Key in your Old Password (if it is the first initiation, the “admin” will be the defaulted one.
2: Enter your New Password
3: Enter your Password again for confirmation; it must be the same as the New Password.
4. Then click on “Next” to get into next installation.

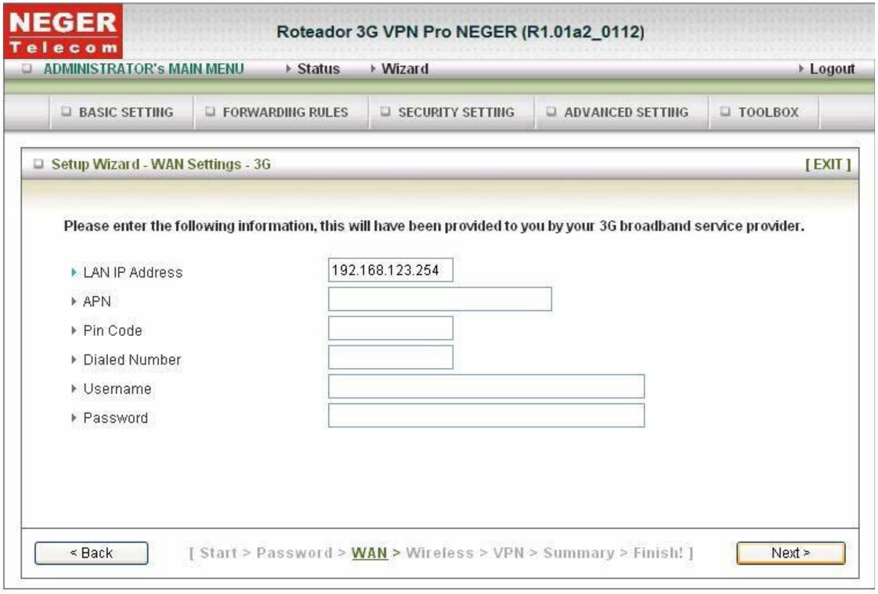
Step 2: Select the WAN internet connection, 3G card, iBurst card or Wired Ethernet port.


NEGER Telecom
Roteador 3G VPN Pro NEGER (R1.01a2_0112)
ADMINISTRATOR's MAIN MENU
Status
Wizard
Logout
BASIC SETTING
FORWARDING RULES
SECURITY SETTING
ADVANCED SETTING
TOOLBOX
[EXIT]
< Back
[Start > Password > WAN > Wireless > VPN > Summary > Finish!]
Next >

Setup Wizard - Please select the type of WAN connection that you want to use

● 3G card
○ iBurst card
○ WAN Ethernet port

Step 3-1: Select 3G WAN Type will be used for Internet connection.


NEGER Telecom
Roteador 3G VPN Pro NEGER (R1.01a2_0112)
ADMINISTRATOR's MAIN MENU
Status
Wizard
Logout
BASIC SETTING
FORWARDING RULES
SECURITY SETTING
ADVANCED SETTING
TOOLBOX
[EXIT]
< Back
[Start > Password > WAN > Wireless > VPN > Summary > Finish!]
Next >

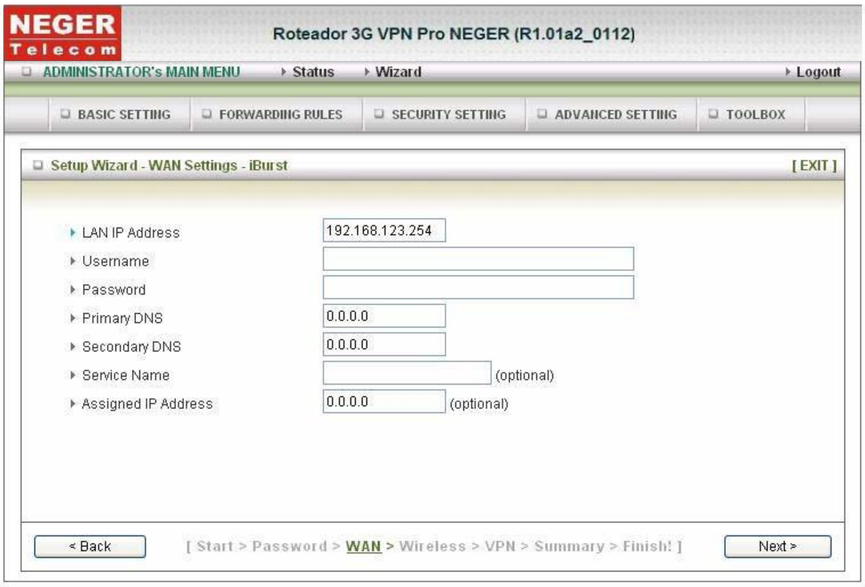
Setup Wizard - WAN Settings - 3G

Please enter the following information, this will have been provided to you by your 3G broadband service provider.

LAN IP Address	192.168.123.254
APN	
Pin Code	
Dialed Number	
Username	
Password	

Enter the information by your 3G broadband service provider.
Click on “Next” button

Step 3-2: Select iBurst WAN Type will be used for Internet connection.

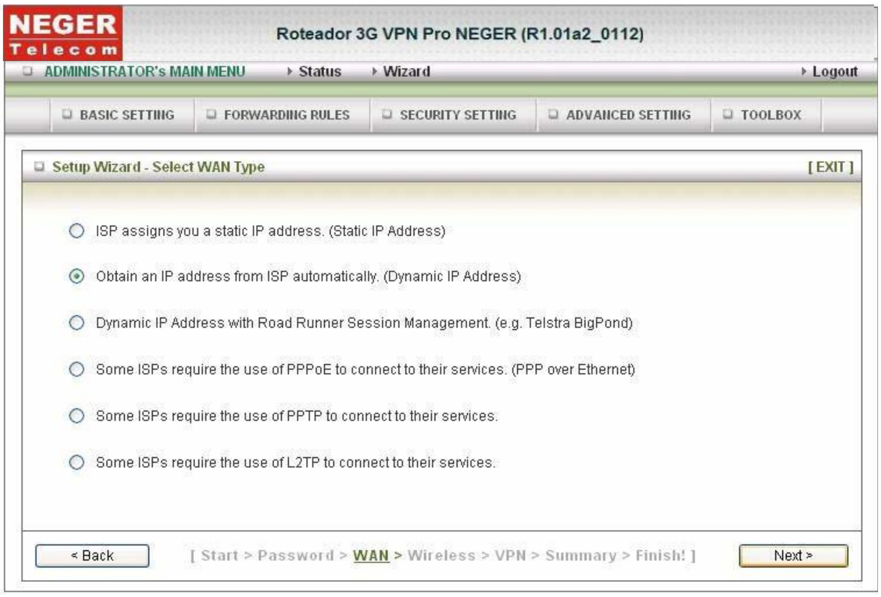

NEGER Telecom
Roteador 3G VPN Pro NEGER (R1.01a2_0112)
ADMINISTRATOR's MAIN MENU
Status
Wizard
Logout
BASIC SETTING
FORWARDING RULES
SECURITY SETTING
ADVANCED SETTING
TOOLBOX
[EXIT]
< Back
[Start > Password > WAN > Wireless > VPN > Summary > Finish!]
Next >

Setup Wizard - WAN Settings - iBurst

LAN IP Address	192.168.123.254
Username	
Password	
Primary DNS	0.0.0.0
Secondary DNS	0.0.0.0
Service Name	(optional)
Assigned IP Address	0.0.0.0 (optional)

Enter the information by your iBurst broadband service provider.
Click on “Next” button

Step 3-3: Select Wired WAN Types will be used for Internet connection


NEGER Telecom
Roteador 3G VPN Pro NEGER (R1.01a2_0112)
ADMINISTRATOR's MAIN MENU
Status
Wizard
Logout
BASIC SETTING
FORWARDING RULES
SECURITY SETTING
ADVANCED SETTING
TOOLBOX
[EXIT]
< Back
[Start > Password > WAN > Wireless > VPN > Summary > Finish!]
Next >

Setup Wizard - Select WAN Type

○ ISP assigns you a static IP address. (Static IP Address)

● Obtain an IP address from ISP automatically. (Dynamic IP Address)

○ Dynamic IP Address with Road Runner Session Management. (e.g. Telstra BigPond)

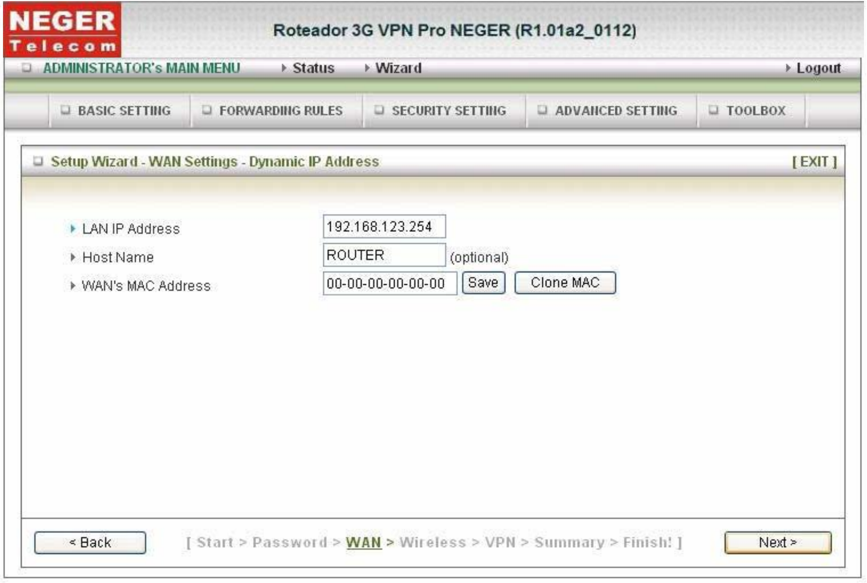
○ Some ISPs require the use of PPPoE to connect to their services. (PPP over Ethernet)

○ Some ISPs require the use of PPTP to connect to their services.

○ Some ISPs require the use of L2TP to connect to their services.

Pick up one of types you preferred to.
Click on "Next" button

Step 4: Configure the LAN IP Address, Host Name and WAN MAC Address.



Setup Wizard - WAN Settings - Dynamic IP Address

LAN IP Address	192.168.123.254
Host Name	ROUTER (optional)
WAN's MAC Address	00-00-00-00-00-00

LAN is short for Local Area Network, and is considered your internal network. These are the IP settings of the LAN interface for the Wireless WAN Mobile Broadband Router, and they may be referred to as Private settings. You may change the LAN IP address if needed. The LAN IP address is private to your internal network and cannot be seen on the Internet.

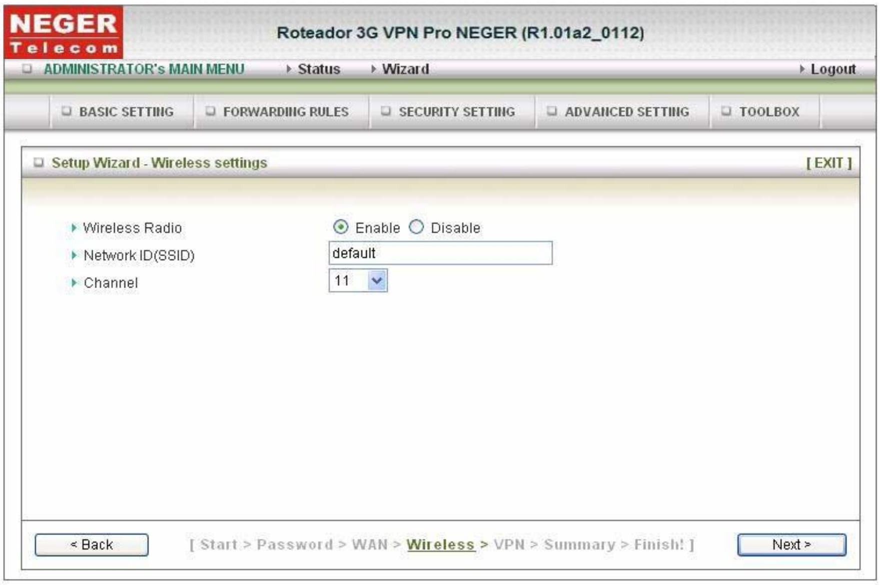
Note: There are 254 addresses available on the Wireless WAN Mobile Broadband Router when using a 255.255.255.0 (Class C) subnet. Example: The router's IP address is 192.168.123.1. The available client IP range is 192.168.123.2 through 192.168.123.254.

1. **LAN IP Address-** The IP address of the LAN interface. The **default** IP address is:

192.168.123.254

2. **Host Name** is optional
3. **WAN's MAC Address-**If you click the Clone MAC button, you will find the MAC address of your NIC shown in WAN's MAC Address
4. Click on "**Next**" to continue.

Step 5: Configure the wireless settings.

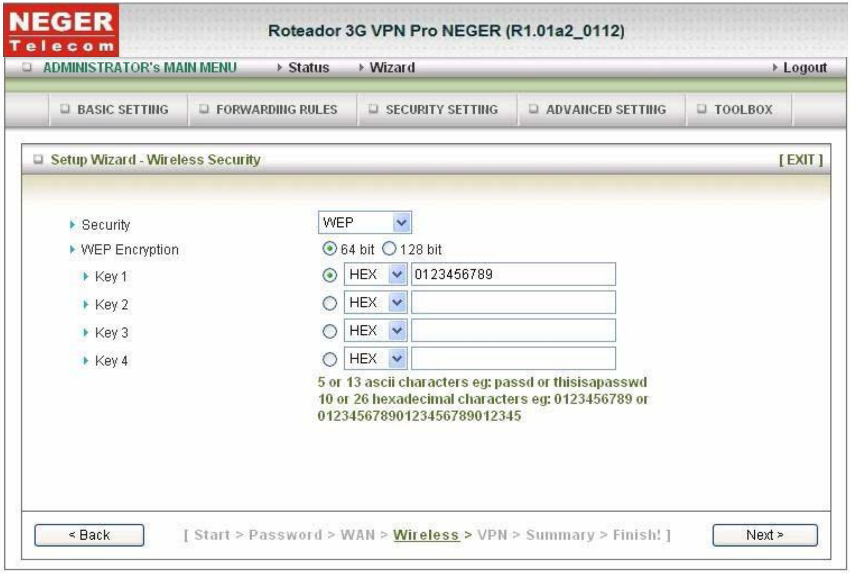

NEGER Telecom
Roteador 3G VPN Pro NEGER (R1.01a2_0112)
ADMINISTRATOR's MAIN MENU
Status
Wizard
Logout
BASIC SETTING
FORWARDING RULES
SECURITY SETTING
ADVANCED SETTING
TOOLBOX
[EXIT]
< Back
[Start > Password > WAN > Wireless > VPN > Summary > Finish!]
Next >

Setup Wizard - Wireless settings

- Wireless Radio: ● Enable ○ Disable
- Network ID(SSID): default
- Channel: 11

1. Select "**Enable**" or "**Disable**". The default setting is "**Enable**".
2. Network ID(SSID) will be defaulted.
3. **Channel**➪ Select Wireless Channel matching to your local area for Wireless connection.
4. Click on "**Next**" to continue.

Step 6: Select the Wireless security method of your wireless configuration.


NEGER Telecom
Roteador 3G VPN Pro NEGER (R1.01a2_0112)
ADMINISTRATOR's MAIN MENU
Status
Wizard
Logout
BASIC SETTING
FORWARDING RULES
SECURITY SETTING
ADVANCED SETTING
TOOLBOX
[EXIT]
< Back
[Start > Password > WAN > Wireless > VPN > Summary > Finish!]
Next >

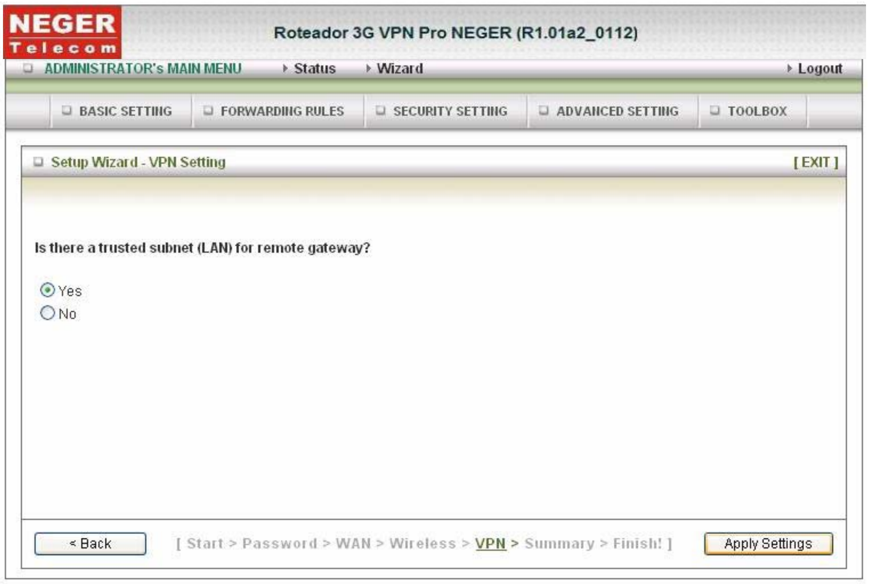
Setup Wizard - Wireless Security

- Security: WEP
- WEP Encryption: ● 64 bit ○ 128 bit
- Key 1: ● HEX 0123456789
- Key 2: ○ HEX
- Key 3: ○ HEX
- Key 4: ○ HEX

5 or 13 ascii characters eg: passd or thisisapasswd
10 or 26 hexadecimal characters eg: 0123456789 or 01234567890123456789012345

1. Select “WEP” Security type and enter the WEP key.
2. Click on “**Next**” to continue.

Step 7: Configure the VPN settings.


NEGER Telecom
Roteador 3G VPN Pro NEGER (R1.01a2_0112)
ADMINISTRATOR's MAIN MENU
Status
Wizard
Logout
BASIC SETTING
FORWARDING RULES
SECURITY SETTING
ADVANCED SETTING
TOOLBOX
Setup Wizard - VPN Setting
[EXIT]
< Back
[Start > Password > WAN > Wireless > VPN > Summary > Finish!]
Apply Settings

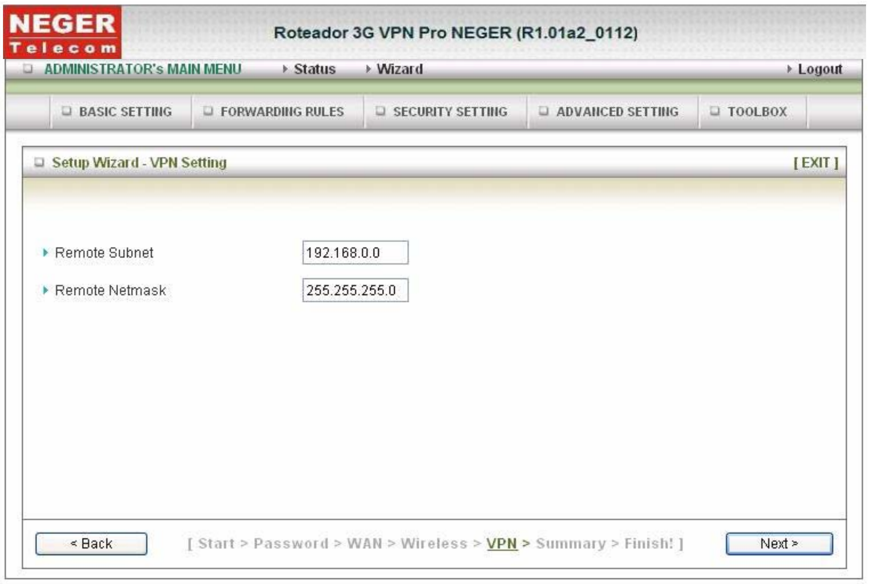
Is there a trusted subnet (LAN) for remote gateway?

● Yes
○ No

The subnet of LAN site of remote VPN gateway, it can be a host, a partial subnet, or the whole subnet of LAN site of remote gateway.

Skip the Step 9, "Remote Subnet settings", if you don't have remote subnet.

Step 8: VPN – Remote Subnet settings


NEGER Telecom
Roteador 3G VPN Pro NEGER (R1.01a2_0112)
ADMINISTRATOR's MAIN MENU
Status
Wizard
Logout
BASIC SETTING
FORWARDING RULES
SECURITY SETTING
ADVANCED SETTING
TOOLBOX
Setup Wizard - VPN Setting
[EXIT]
< Back
[Start > Password > WAN > Wireless > VPN > Summary > Finish!]
Next >

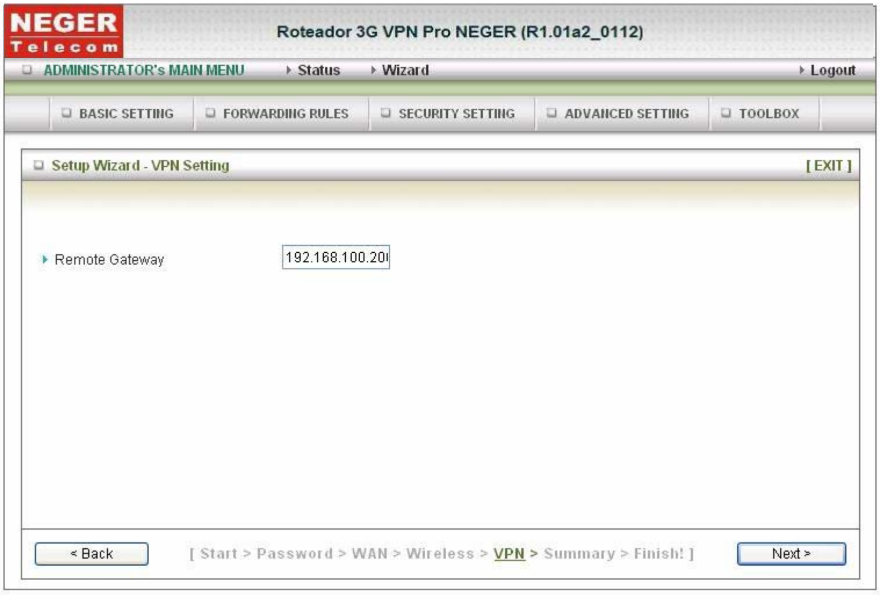
Remote Subnet: 192.168.0.0

Remote Netmask: 255.255.255.0

Remote Subnet: The subnet of LAN site of remote VPN gateway, it can be a host, a partial subnet, and the whole subnet of LAN site of remote gateway.

Remote Netmask: Remote Netmask combined with remote subnet to form a subnet domain of remote end.

Step 9: VPN – Remote Gateway Setting



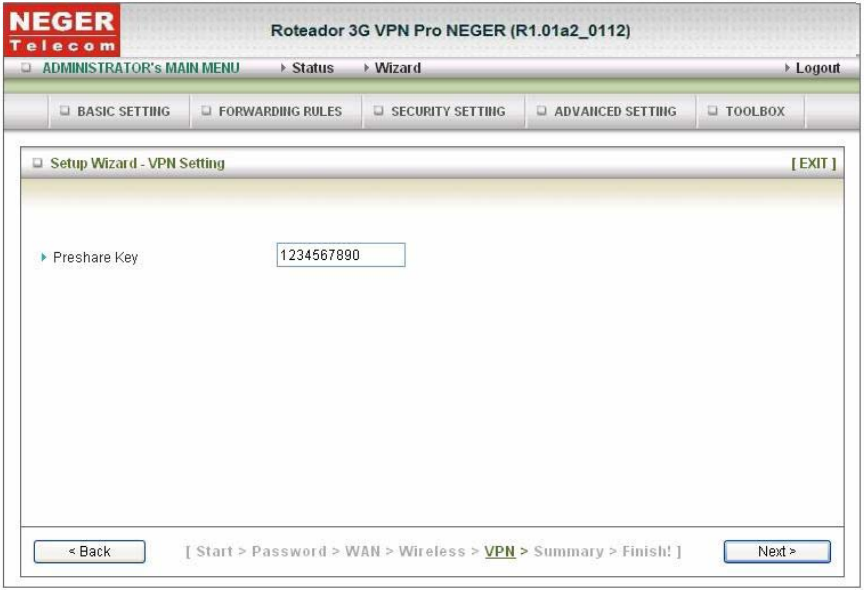
NEGER Telecom
Roteador 3G VPN Pro NEGER (R1.01a2_0112)
ADMINISTRATOR's MAIN MENU
Status
Wizard
Logout
BASIC SETTING
FORWARDING RULES
SECURITY SETTING
ADVANCED SETTING
TOOLBOX
< Back
[Start > Password > WAN > Wireless > VPN > Summary > Finish!]
Next >

Setup Wizard - VPN Setting [EXIT]

Remote Gateway: 192.168.100.20

Enter the IP address of remote VPN gateway.

Step 10: VPN – Preshare Key



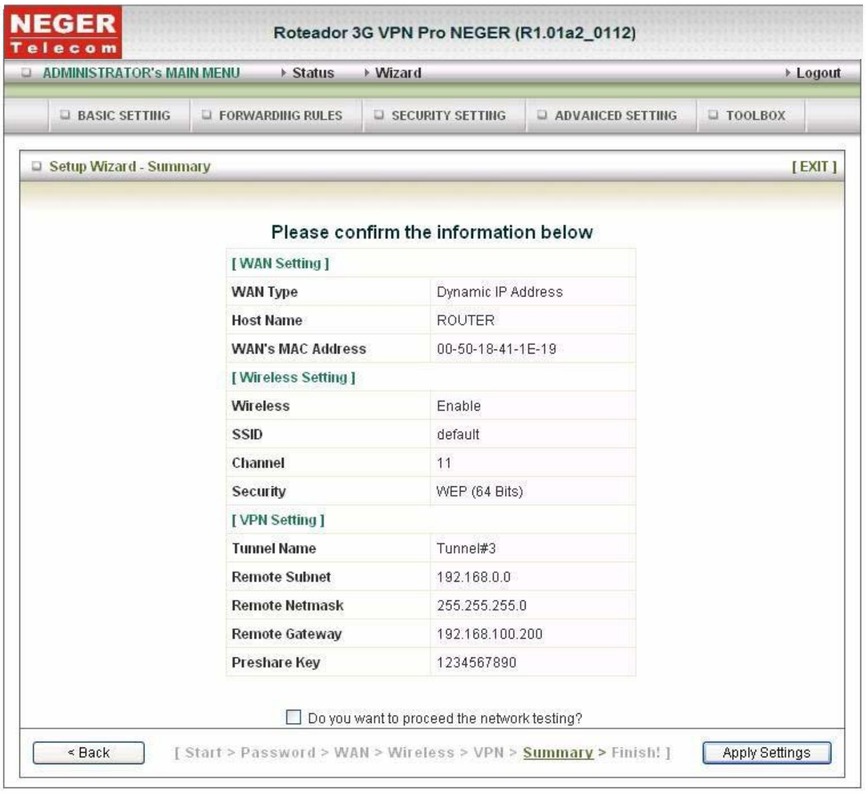
NEGER Telecom
Roteador 3G VPN Pro NEGER (R1.01a2_0112)
ADMINISTRATOR's MAIN MENU
Status
Wizard
Logout
BASIC SETTING
FORWARDING RULES
SECURITY SETTING
ADVANCED SETTING
TOOLBOX
< Back
[Start > Password > WAN > Wireless > VPN > Summary > Finish!]
Next >

Setup Wizard - VPN Setting [EXIT]

Preshare Key: 1234567890

1. This is a first key that supports IKE mechanism of both VPN gateways for negotiating further security keys. The pre-shared key must be same for both end gateways.
2. The maximal length is 32.

Step 11: Summary



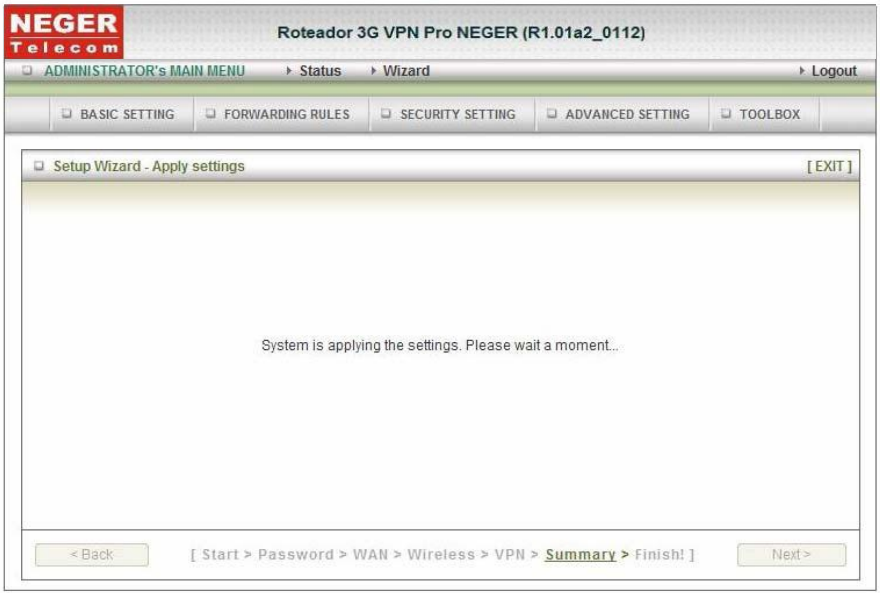
Please confirm the information below

[WAN Setting]	
WAN Type	Dynamic IP Address
Host Name	ROUTER
WAN's MAC Address	00-50-18-41-1E-19
[Wireless Setting]	
Wireless	Enable
SSID	default
Channel	11
Security	WEP (64 Bits)
[VPN Setting]	
Tunnel Name	Tunnel#3
Remote Subnet	192.168.0.0
Remote Netmask	255.255.255.0
Remote Gateway	192.168.100.200
Preshare Key	1234567890

□ Do you want to proceed the network testing?

Click on the "**Apply Settings**" button

Step 12: System is applying.

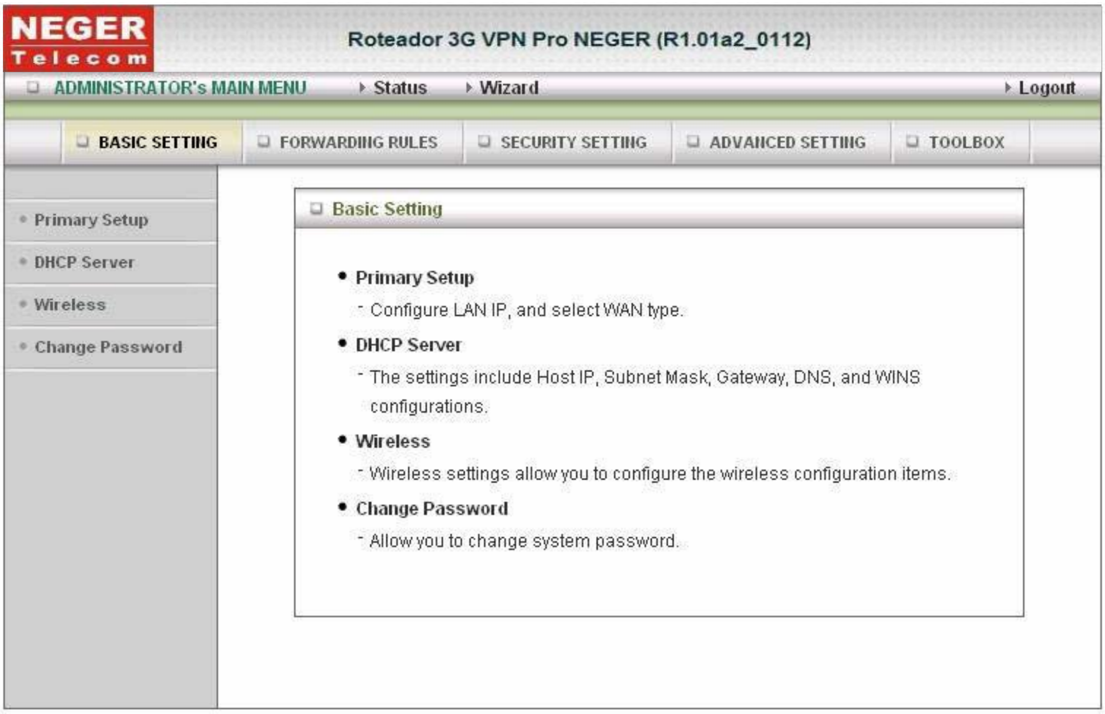

NEGER Telecom
Roteador 3G VPN Pro NEGER (R1.01a2_0112)
ADMINISTRATOR's MAIN MENU
Status
Wizard
Logout
BASIC SETTING
FORWARDING RULES
SECURITY SETTING
ADVANCED SETTING
TOOLBOX
Setup Wizard - Apply settings
[EXIT]
< Back
[Start > Password > WAN > Wireless > VPN > Summary > Finish!]
Next >

System is applying the settings. Please wait a moment...

Click "Next" button to back the Status Page.

3.2. Administrator’s Main Menu

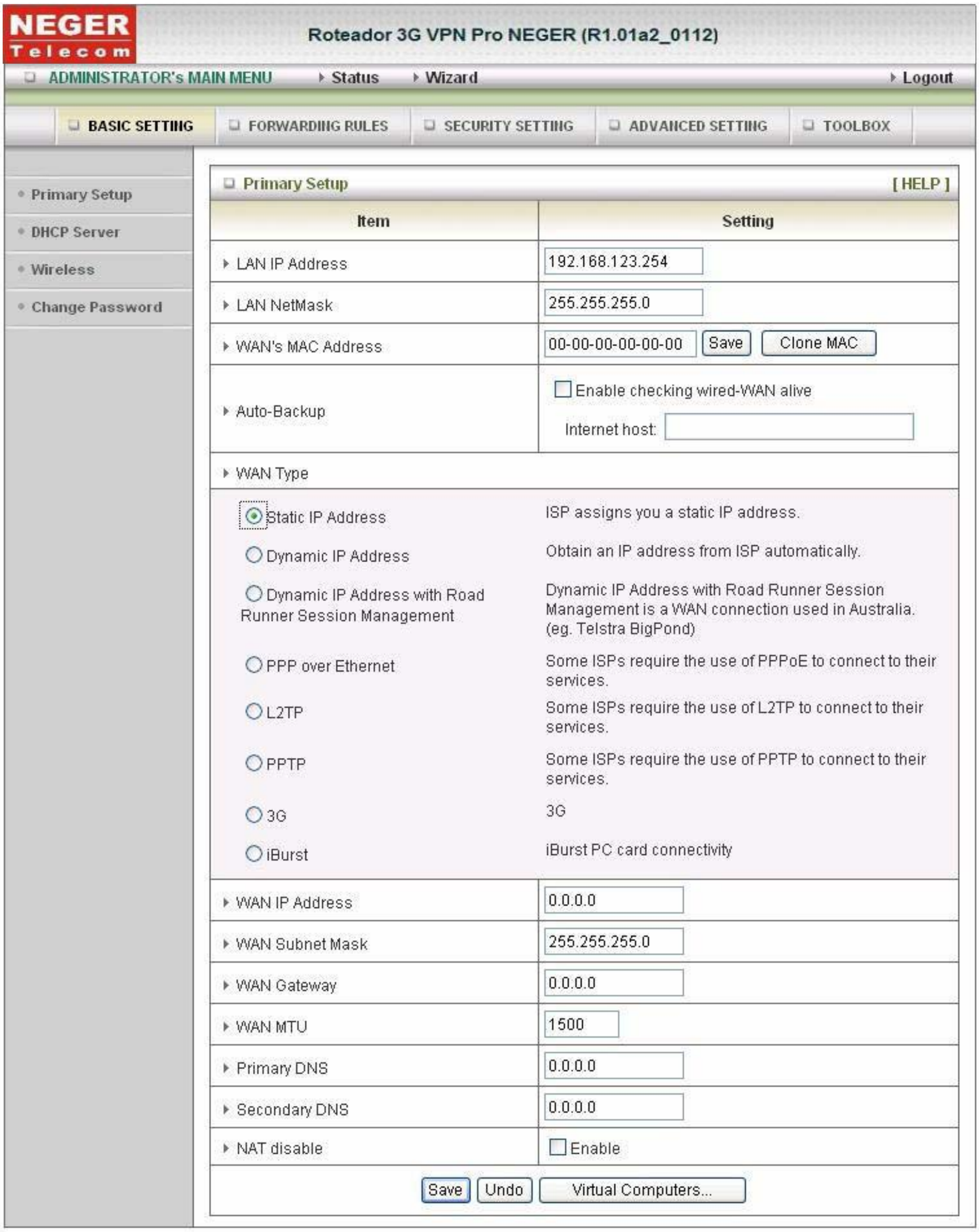
3.2.1 Basic Setting



Basic Setting

- Primary Setup
  - Configure LAN IP, and select WAN type.
- DHCP Server
  - The settings include Host IP, Subnet Mask, Gateway, DNS, and WINS configurations.
- Wireless
  - Wireless settings allow you to configure the wireless configuration items.
- Change Password
  - Allow you to change system password.

3.2.1.1 Primary Setup - WAN Type, Virtual Computers



Primary Setup

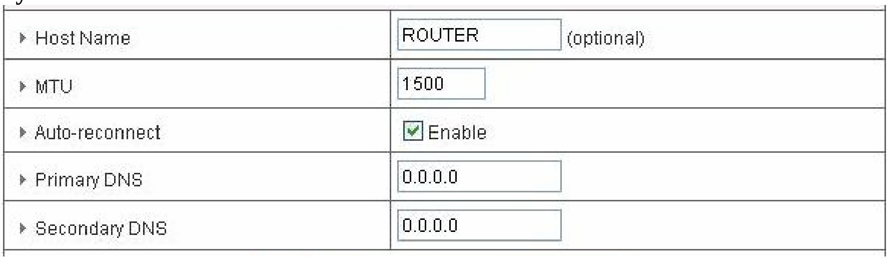
Item	Setting
LAN IP Address	192.168.123.254
LAN NetMask	255.255.255.0
WAN's MAC Address	00-00-00-00-00-00 Save Clone MAC
Auto-Backup	□ Enable checking wired-WAN alive Internet host:
WAN Type	
● Static IP Address	ISP assigns you a static IP address.
○ Dynamic IP Address	Obtain an IP address from ISP automatically.
○ Dynamic IP Address with Road Runner Session Management	Dynamic IP Address with Road Runner Session Management is a WAN connection used in Australia. (eg. Telstra BigPond)
○ PPP over Ethernet	Some ISPs require the use of PPPoE to connect to their services.
○ L2TP	Some ISPs require the use of L2TP to connect to their services.
○ PPTP	Some ISPs require the use of PPTP to connect to their services.
○ 3G	3G
○ iBurst	iBurst PC card connectivity
WAN IP Address	0.0.0.0
WAN Subnet Mask	255.255.255.0
WAN Gateway	0.0.0.0
WAN MTU	1500
Primary DNS	0.0.0.0
Secondary DNS	0.0.0.0
NAT disable	□ Enable

1. **LAN IP Address:** the local IP address of this device. The computers on your network must use the LAN IP address of your product as their Default Gateway. You can change it if necessary.
2. **LAN NetMask:** LAN Netmask combined with LAN subnet to form a subnet domain.
3. **WAN's MAC Address:** The default MAC Address is set to the WAN's physical interface MAC address on the Router.

4. **Clone – WAN's MAC Address:** This feature will copy the MAC address of the Ethernet card, and replace the WAN MAC address of the Router with this Ethernet card MAC address. It is not recommended that you change the default MAC address unless required by your ISP.
5. **Auto-Backup:** The WAN type will be change to 3G automatically, if the wired-WAN is defunct.
6. **WAN Type**: WAN connection type of your ISP. You can click WAN Type Combo button to choose a correct one from the following options:

Static IP Address:
WAN IP Address, Subnet Mask, Gateway, Primary and Secondary DNS: enter the proper setting provided by your ISP.

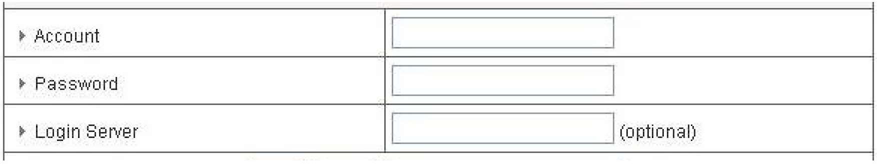
Dynamic IP Address:



Host Name	ROUTER (optional)
MTU	1500
Auto-reconnect	☑ Enable
Primary DNS	0.0.0.0
Secondary DNS	0.0.0.0

1. Host Name: optional, required by some ISPs, for example, @Home.
2. MTU(Maximum Transmission Unit): Most ISP offers MTU value to users. The most common MTU value is 1492.
3. Auto-reconnect: this feature enables this product to renew your IP address automatically when the lease time is expiring-- even when the system is idle.

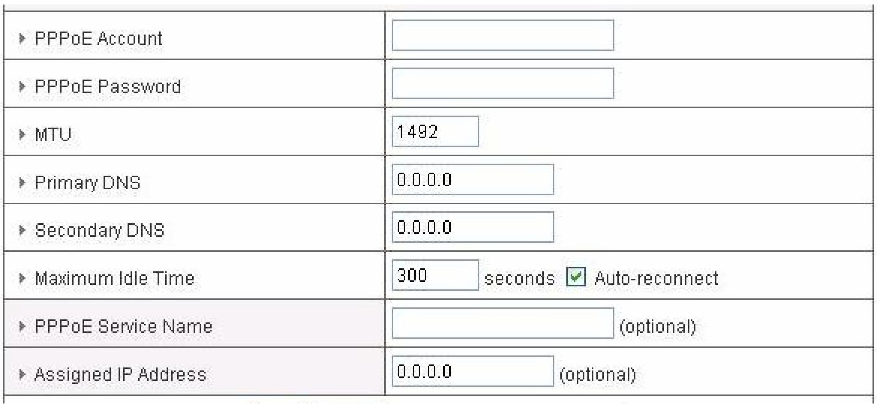
Dynamic IP Address with Road Runner



Account	
Password	
Login Server	(optional)

1. Account and Password: the account and password your ISP assigned to you.

PPP over Ethernet



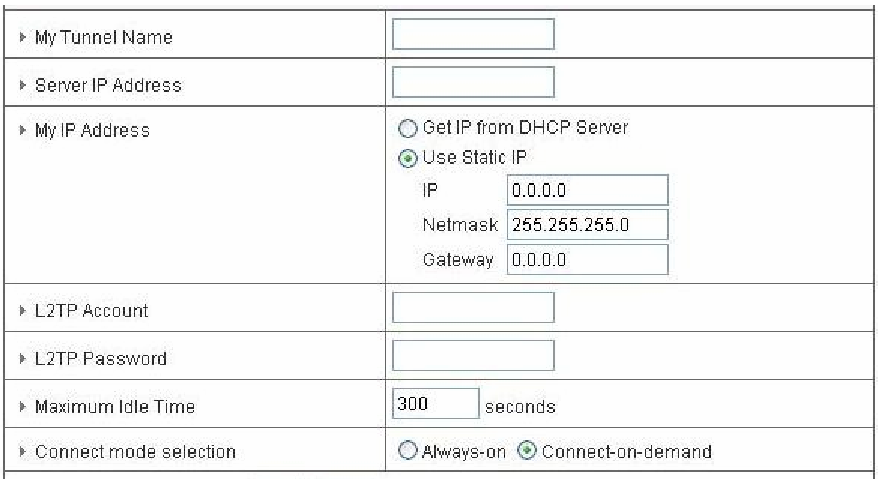
PPPoE Account	
PPPoE Password	
MTU	1492
Primary DNS	0.0.0.0
Secondary DNS	0.0.0.0
Maximum Idle Time	300 seconds ☑ Auto-reconnect
PPPoE Service Name	(optional)
Assigned IP Address	0.0.0.0 (optional)

1. PPPoE Account and Password: the account and password your ISP assigned to you. For security, this field appears blank. If you don't want to change the password, leave it empty.
2. Maximum Transmission Unit (MTU): Most ISP offers MTU value to users. The most common MTU value is 1492.
3. Maximum Idle Time: the amount of time of inactivity before disconnecting your PPPoE

session. Set it to zero or enable Auto-reconnect to disable this feature.

4. Auto Reconnect (Always-on): The device will link with ISP until the connection is established.
5. PPPoE Service Name: optional. Input the service name if your ISP requires it. Otherwise, leave it blank.

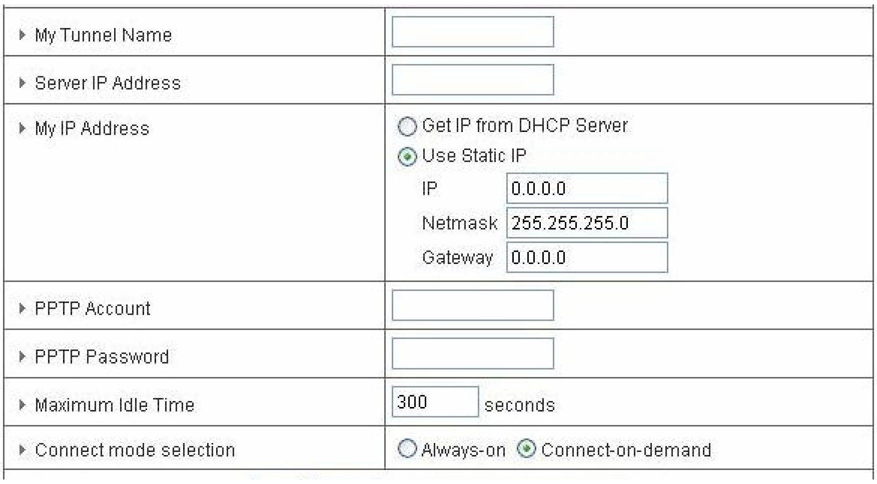
L2TP



My Tunnel Name	
Server IP Address	
My IP Address	○ Get IP from DHCP Server ● Use Static IP IP 0.0.0.0 Netmask 255.255.255.0 Gateway 0.0.0.0
L2TP Account	
L2TP Password	
Maximum Idle Time	300 seconds
Connect mode selection	○ Always-on ● Connect-on-demand

1. First, please check your ISP assigned and Select Static IP Address or Dynamic IP Address. For example: Use Static, the private IP address, subnet mask and Gateway are your ISP assigned to you.
2. Server IP Address: the IP address of the L2TP server.
3. PPTP Account and Password: the account and password your ISP assigned to you. If you don't want to change the password, keep it empty.
4. Maximum Idle Time: the time of no activity to disconnect your L2TP session. Set it to zero or enable Always-on to disable this feature. If Always-on is enabled, this product will connect to ISP automatically, after system is restarted or connection is dropped.
5. Connect mode selection: There are 2 modes to select:
   Always-on: The device will link with ISP until the connection is established.
   Connect-on-demand: The device will link up with ISP when the clients send outgoing packets.

PPTP



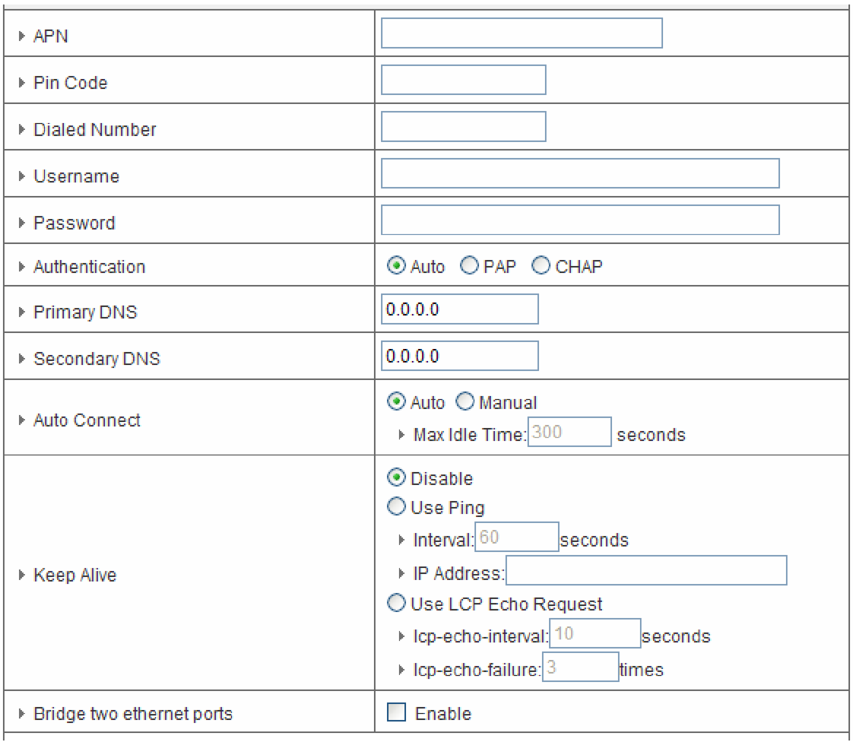
My Tunnel Name	
Server IP Address	
My IP Address	○ Get IP from DHCP Server ● Use Static IP IP 0.0.0.0 Netmask 255.255.255.0 Gateway 0.0.0.0
PPTP Account	
PPTP Password	
Maximum Idle Time	300 seconds
Connect mode selection	○ Always-on ● Connect-on-demand

1. First, please check your ISP assigned and Select Static IP Address or Dynamic IP Address. For example: Use Static, the private IP address, subnet mask and Gateway are your ISP

assigned to you.

2. Server IP Address: the IP address of the PPTP server.
3. PPTP Account and Password: the account and password your ISP assigned to you. If you don't want to change the password, keep it empty.
4. Maximum Idle Time: the time of no activity to disconnect your PPTP session. Set it to zero or enable Always-on to disable this feature. If Always-on is enabled, this product will connect to ISP automatically, after system is restarted or connection is dropped.
5. Connection mode selection: There are 2 modes to select:
   Always-on: The device will link with ISP until the connection is established.
   Connect-on-demand: The device will link up with ISP when the clients send outgoing packets.

3G



APN	
Pin Code	
Dialed Number	
Username	
Password	
Authentication	● Auto ○ PAP ○ CHAP
Primary DNS	0.0.0.0
Secondary DNS	0.0.0.0
Auto Connect	● Auto ○ Manual Max Idle Time: 300 seconds
Keep Alive	● Disable ○ Use Ping Interval: 60 seconds IP Address: ○ Use LCP Echo Request lcp-echo-interval: 10 seconds lcp-echo-failure: 3 times
Bridge two ethernet ports	□ Enable

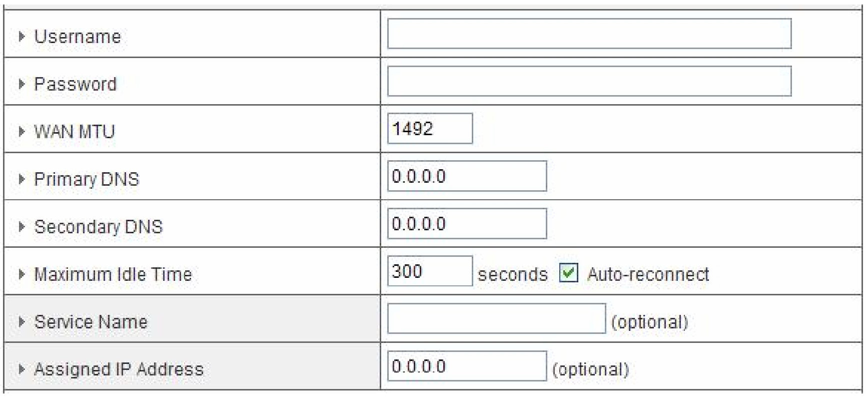
For 3G WAN Networking. The WAN fields may not be necessary for your connection. The information on this page will only be used when your service provider requires you to enter a User Name and Password to connect to the 3G network.

Please refer to your documentation or service provider for additional information.

1. APN: Enter the APN for your PC card here.
2. Pin Code: Enter the Pin Code for your SIM card
3. Dial-Number: This field should not be altered except when required by your service provider.
4. User Name: Enter the new User Name for your PC card here.
5. Password: Enter the new Password for your PC card here.
6. Primary DNS: This feature allows you to assign a Primary DNS Server（Optional）
7. Secondary DNS: This feature allows you to assign a Secondary DNS Server（Optional）
8. Auto Connect: There are 2 modes to select:
   Auto: The device will link up with ISP when the clients send outgoing packets.
   Manual: Manually: The device will not make the link until someone clicks the connect-button in the Status-page.
9. Maximum Idle Time: The Connection will be broken when the idle time arrives.

10. Keep Alive: There are 3 modes to select:
    Disable / Use Ping /Use LCP Echo Request
11. Bridge two ethernet ports: Bridge the two ports, wired WAN and wired LAN. So we have 2 LAN ports and don't have wired WAN port.

iBurst



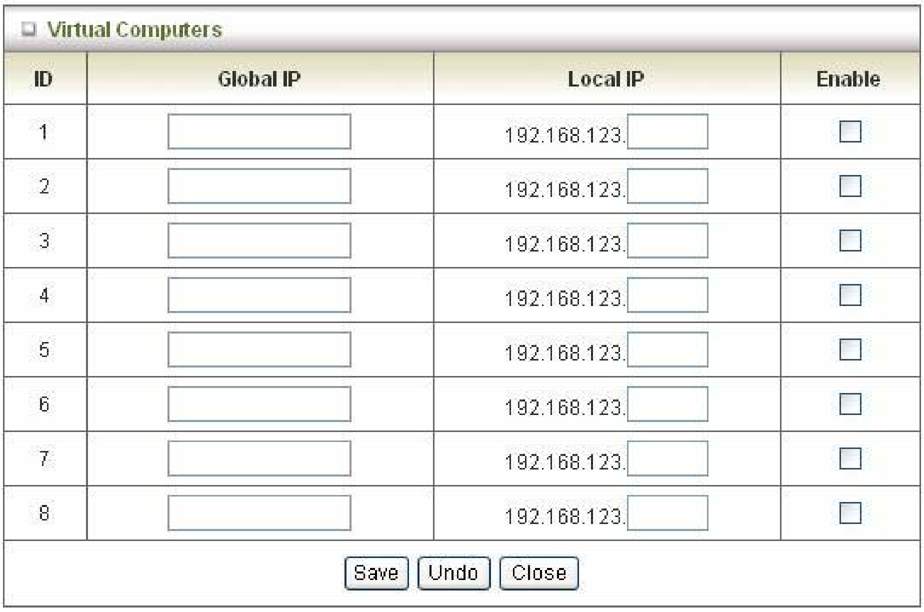
Username	
Password	
WAN MTU	1492
Primary DNS	0.0.0.0
Secondary DNS	0.0.0.0
Maximum Idle Time	300 seconds ☑ Auto-reconnect
Service Name	(optional)
Assigned IP Address	0.0.0.0 (optional)

For iBurst PC card(3G) WAN Networking. The WAN fields may not be necessary for your connection. The information on this page will only be used when your service provider requires you to enter a User Name and Password to connect to the 3G network.

Please refer to your documentation or service provider for additional information.

1. User Name: Enter the new User Name for your PC card here.
2. Password: Enter the new Password for your PC card here.
3. Primary DNS: This feature allows you to assign a Primary DNS Server（Optional）
4. Secondary DNS: This feature allows you to assign a Secondary DNS Server（Optional）
5. Maximum Idle Time: The Connection will be broken when the idle time arrives.
6. Auto-reconnect: The device will link up with ISP when the clients send outgoing packets.

3.2.1.2 Virtual Computers (Only for Static and dynamic IP address Wan type)



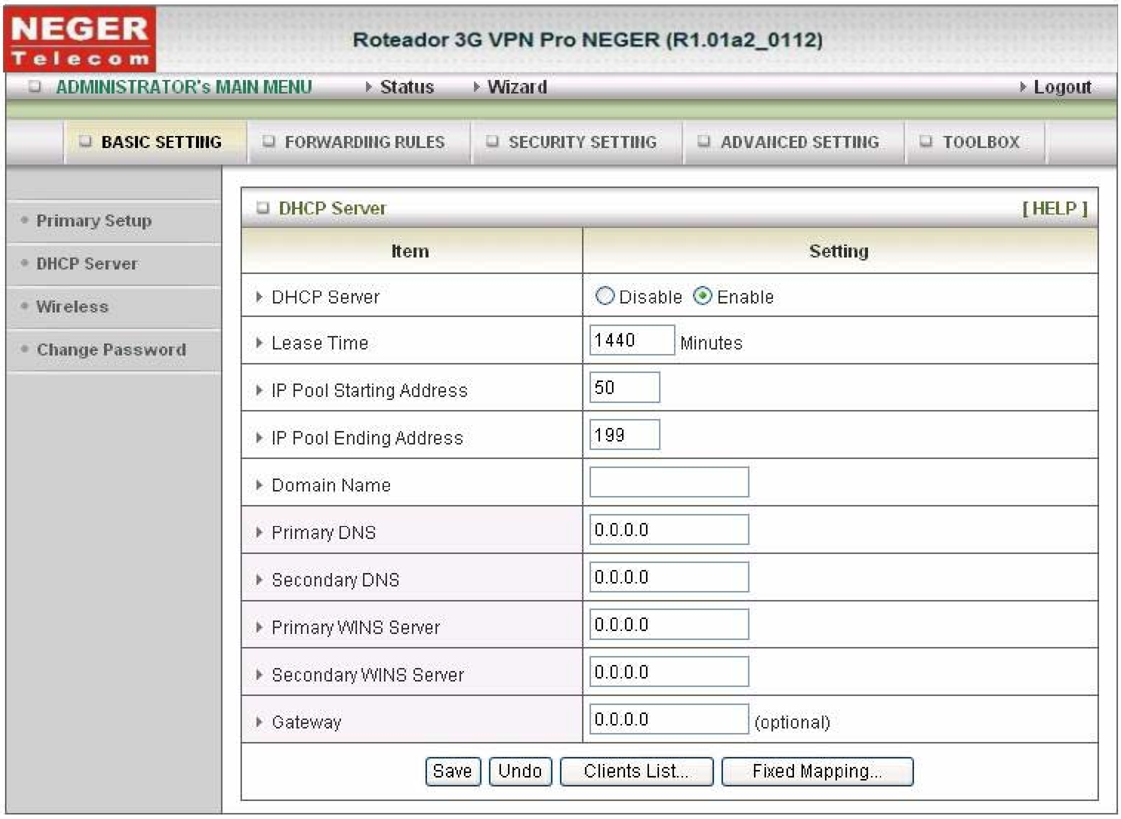
Virtual Computers

ID	Global IP	Local IP	Enable
1		192.168.123.	□
2		192.168.123.	□
3		192.168.123.	□
4		192.168.123.	□
5		192.168.123.	□
6		192.168.123.	□
7		192.168.123.	□
8		192.168.123.	□

Virtual Computer enables you to use the original NAT feature, and allows you to setup the one-to-one mapping of multiple global IP address and local IP address.

1. Global IP: Enter the global IP address assigned by your ISP.
2. Local IP: Enter the local IP address of your LAN PC corresponding to the global IP address.
3. Enable: Check this item to enable the Virtual Computer feature.

3.2.1.3 DHCP Server



DHCP Server

Item	Setting
DHCP Server	○ Disable ● Enable
Lease Time	1440 Minutes
IP Pool Starting Address	50
IP Pool Ending Address	199
Domain Name	
Primary DNS	0.0.0.0
Secondary DNS	0.0.0.0
Primary WINS Server	0.0.0.0
Secondary WINS Server	0.0.0.0
Gateway	0.0.0.0 (optional)

Press **“More>>”,**

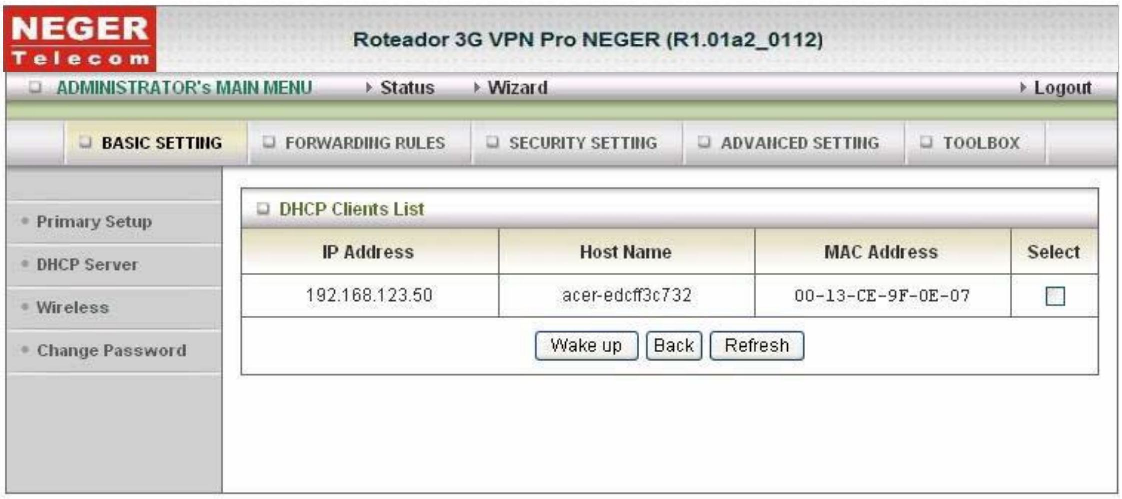
1. **DHCP Server:** Choose either **Disable** or **Enable**
2. **Lease Time:** DHCP lease time to the DHCP client
3. **IP Pool Starting/Ending Address:** Whenever there is a request, the DHCP server will automatically allocate an unused IP address from the IP address pool to the requesting computer. You must specify the starting / ending address of the IP address pool
4. **Domain Name:** Optional, this information will be passed to the client
5. **Primary DNS/Secondary DNS:** Optional, This feature allows you to assign a DNS Servers
6. **Primary WINS/Secondary WINS:** Optional, this feature allows you to assign a WINS Servers
7. **Gateway:** Optional, Gateway Address would be the IP address of an alternate Gateway. This function enables you to assign another gateway to your PC, when DHCP server offers an IP to your PC.
8. **Fixed Mapping:** Reference the page “MAC Address Control”.

After you finish your selection then

Click on **“Save”** to store what you just pick or click “**Undo”** to give up

DHCP Clients List

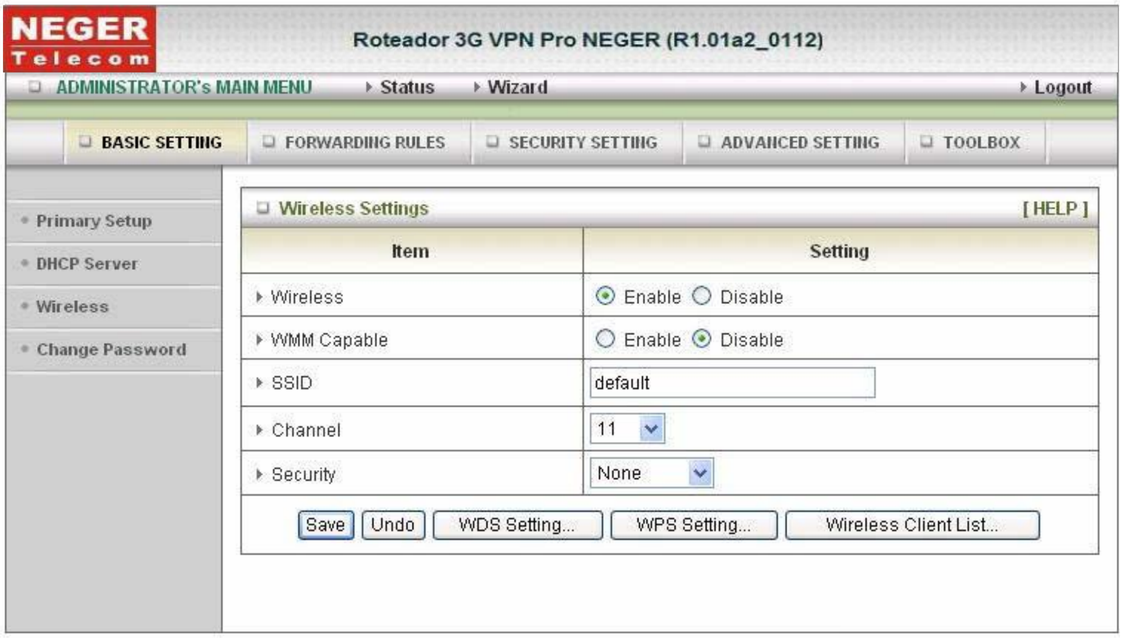
The list of DHCP clients are show here.



DHCP Clients List

IP Address	Host Name	MAC Address	Select
192.168.123.50	acer-edcff3c732	00-13-CE-9F-0E-07	□

3.2.1.4 Wireless Settings



Item	Setting
Wireless	● Enable ○ Disable
WMM Capable	○ Enable ● Disable
SSID	default
Channel	11
Security	None

Wireless settings allow you to set the wireless configuration items.

1. **Wireless:** *Enable* is the default**.** Selecting this option will allow you to set your Wireless Access Point (WAP) settings.
2. **WMM Capable:** *Disable* is the default**.** WMM® Quality of Service is a set of features for Wi-Fi networks that improve the user experience for audio, video, and voice applications by prioritizing data traffic.
3. **SSID:** Service Set Identifier (SSID) is the name designated for a specific wireless local area network (WLAN). The SSID's factory default setting is *default*. The SSID can be easily changed to establish a new wireless network.(Note: SSID names may contain up to 32 ASCII characters).
4. **Channel:** *Auto* is the default. Devices on the network must share the same channel. (Note: Wireless adapters automatically scan and match the wireless settings. You may also select the channel you wish to use).
5. **Security:** You may select from several security types to use: None, WEP, 802.1X, WPA-PSK, WPA, WPA2PSK, WPA2.

None:
No Wi-Fi security settings are on the device.

WEP:
When you enable the 128 or 64 bit WEP key security, please select one WEP key to be used and input 26 or 10 hexadecimal (0, 1, 2…8, 9, A, B…F) digits.

802.1X
Check Box was used to switch the function of the 802.1X. When the 802.1X function is enabled, the Wireless user must authenticate to this router first to use the Network service.

1. RADIUS Server IP: IP address or the 802.1X server’s domain-name.
2. RADIUS port: The default port is 1812.
3. RADIUS Shared Key: Key value shared by the RADIUS server and this router. This key

value is consistent with the key value in the RADIUS server.

WPA-PSK

1. Select Encryption type, TKIP or AES
2. Passphrase: The length of pre-share key is from 8 to 63.
3. Fill in the key, Ex 12345678

WPA

Check Box was used to switch the function of the WPA. When the WPA function is enabled, the Wireless user must authenticate to this router first to use the Network service, RADIUS Server.

1. IP address or the 802.1X server's domain-name.
2. Select Encryption and key in RADIUS Server IP/ Port / Shared Key.
3. Key value shared by the RADIUS server and this router. This key value is consistent with the key value in the RADIUS server.

WPA2-PSK

1. Select Encryption type, TKIP or AES.
2. Passphrase: The length of pre-share key is from 8 to 63.
3. Fill in the key, Ex 12345678.

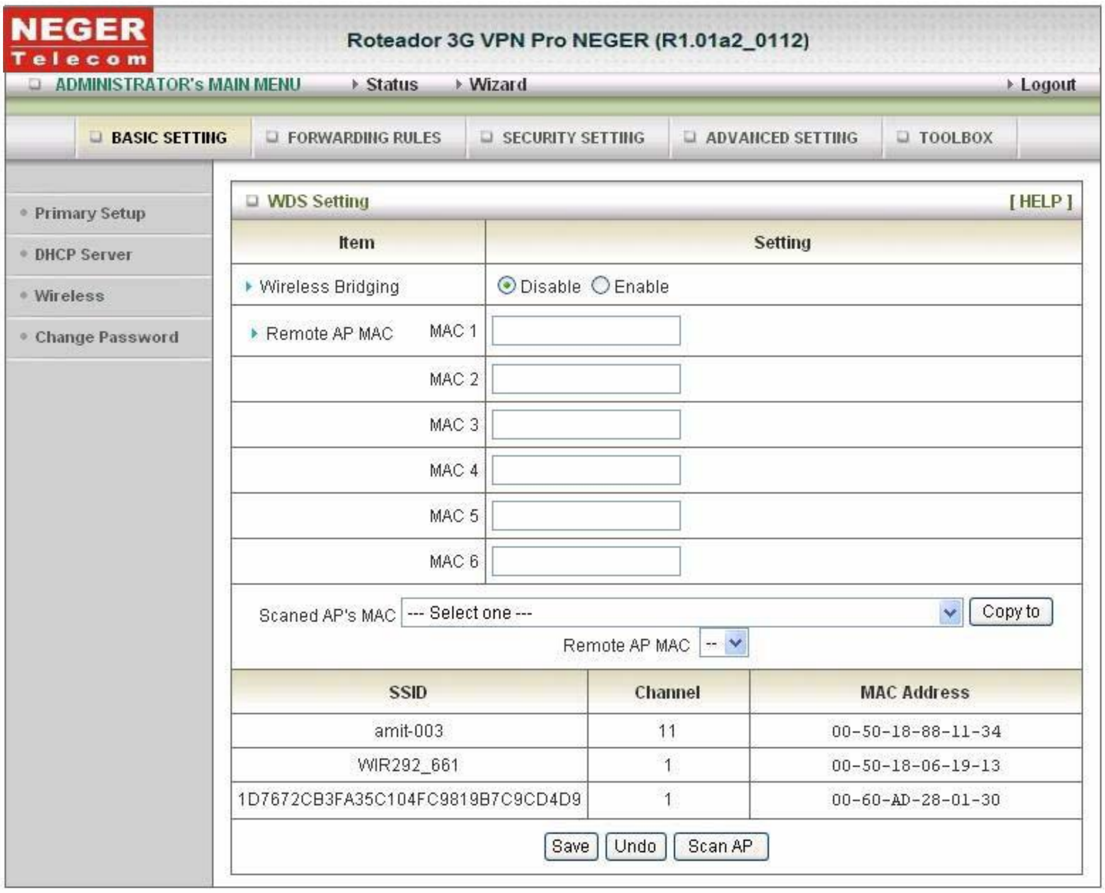
WPA2

Check Box was used to switch the function of the WPA2. When the WPA2 function is enabled, the Wireless user must authenticate to this router first to use the Network service, RADIUS Server.

1. IP address or the 802.1X server's domain-name.
2. Select Encryption and key in RADIUS Server IP/ Port / Shared Key.
3. Key value shared by the RADIUS server and this router. This key value is consistent with the key value in the RADIUS server.

WDS (Wireless Distribution System) Setting

WDS operation as defined by the IEEE802.11 standard has been made available. Using WDS it is possible to wirelessly connect Access Points, and in doing so extend a wired infrastructure to locations where cabling is not possible or inefficient to implement.



Item	Setting
Wireless Bridging	● Disable ○ Enable
Remote AP MAC MAC 1	
MAC 2	
MAC 3	
MAC 4	
MAC 5	
MAC 6	

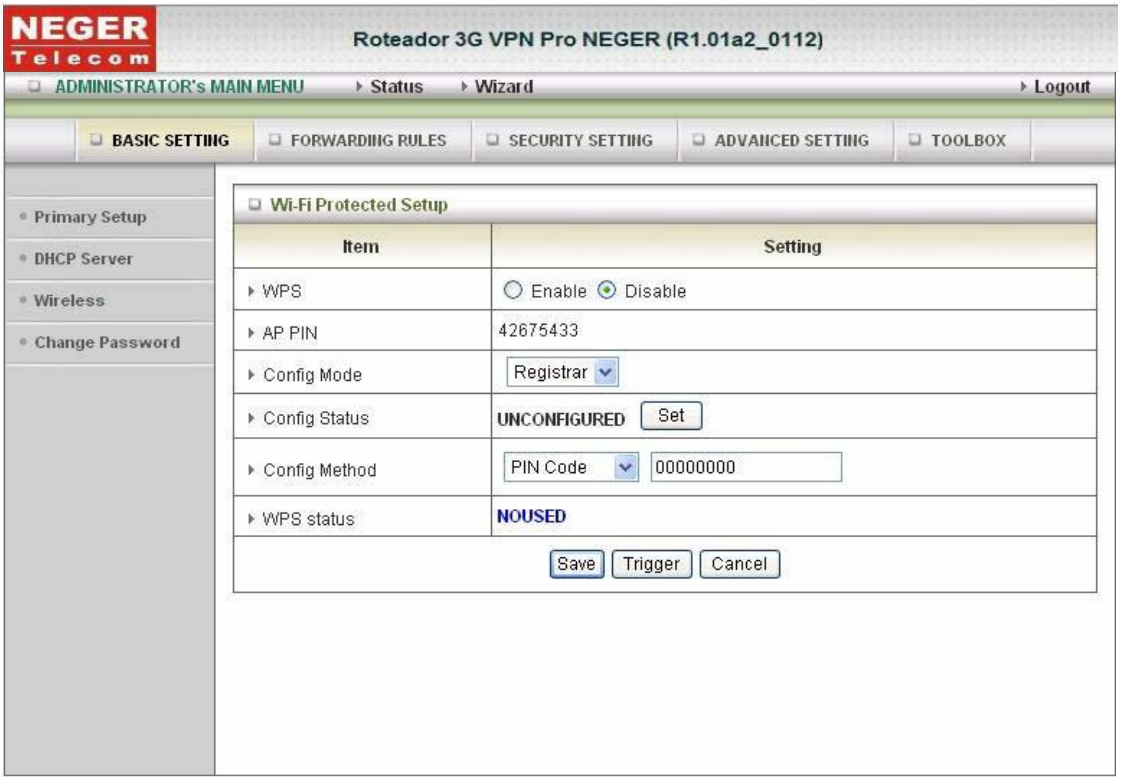
Scaned AP's MAC --- Select one --- Copy to

Remote AP MAC --

SSID	Channel	MAC Address
amit-003	11	00-50-18-88-11-34
WIR292_661	1	00-50-18-06-19-13
1D7672CB3FA35C104FC9819B7C9CD4D9	1	00-60-AD-28-01-30

WPS(Wi-Fi Protection Setup)

WPS is Wi-Fi Protection Setup which is similar to WCN-NET and offers safe and easy way in Wireless Connection.

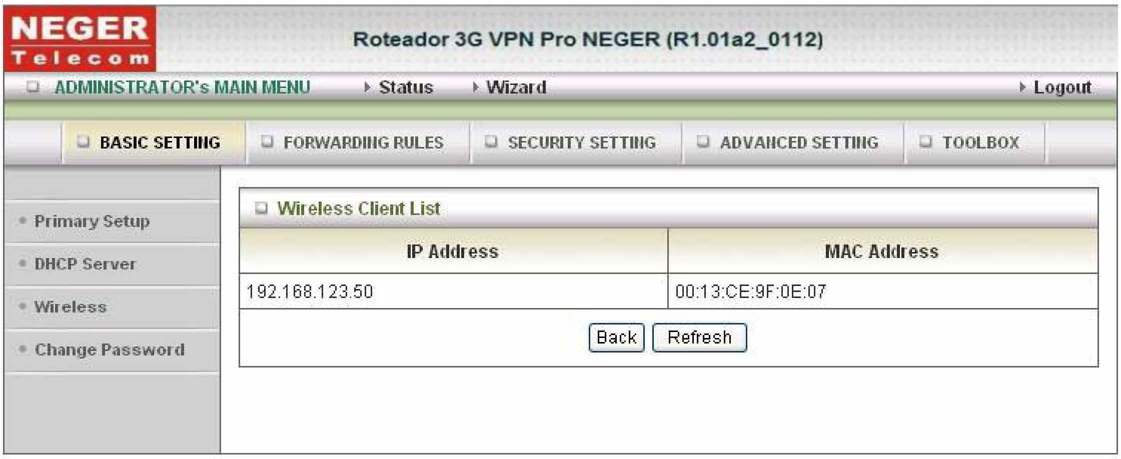


Wi-Fi Protected Setup

Item	Setting
WPS	○ Enable ● Disable
AP PIN	42675433
Config Mode	Registrar
Config Status	UNCONFIGURED Set
Config Method	PIN Code 00000000
WPS status	NOUSED

Wireless Client List

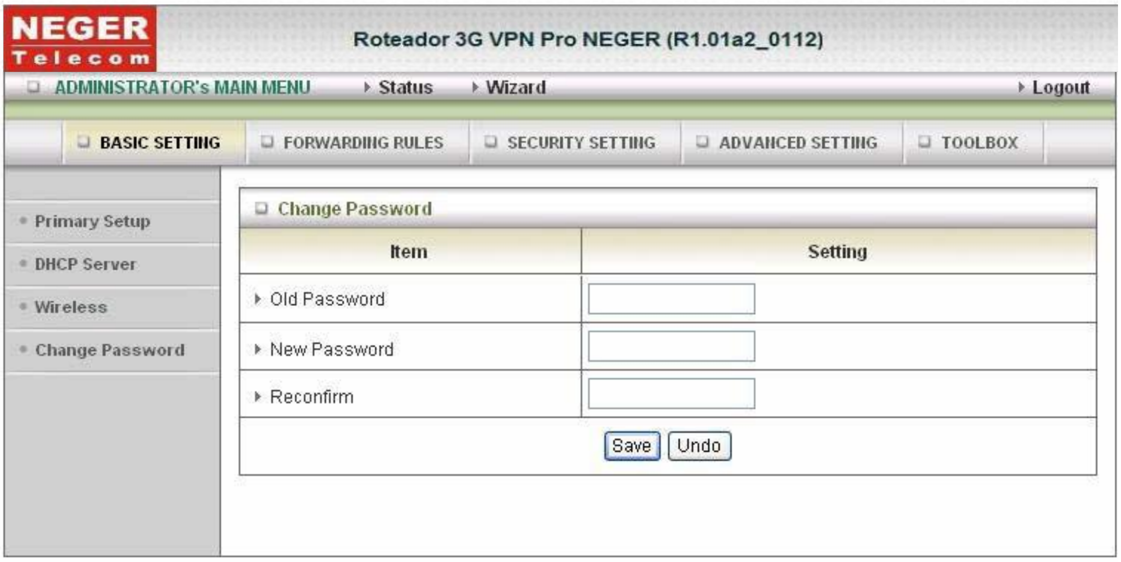
The list of wireless client is shows here.



Wireless Client List

IP Address	MAC Address
192.168.123.50	00:13:CE:9F:0E:07

3.2.1.5 Change Password



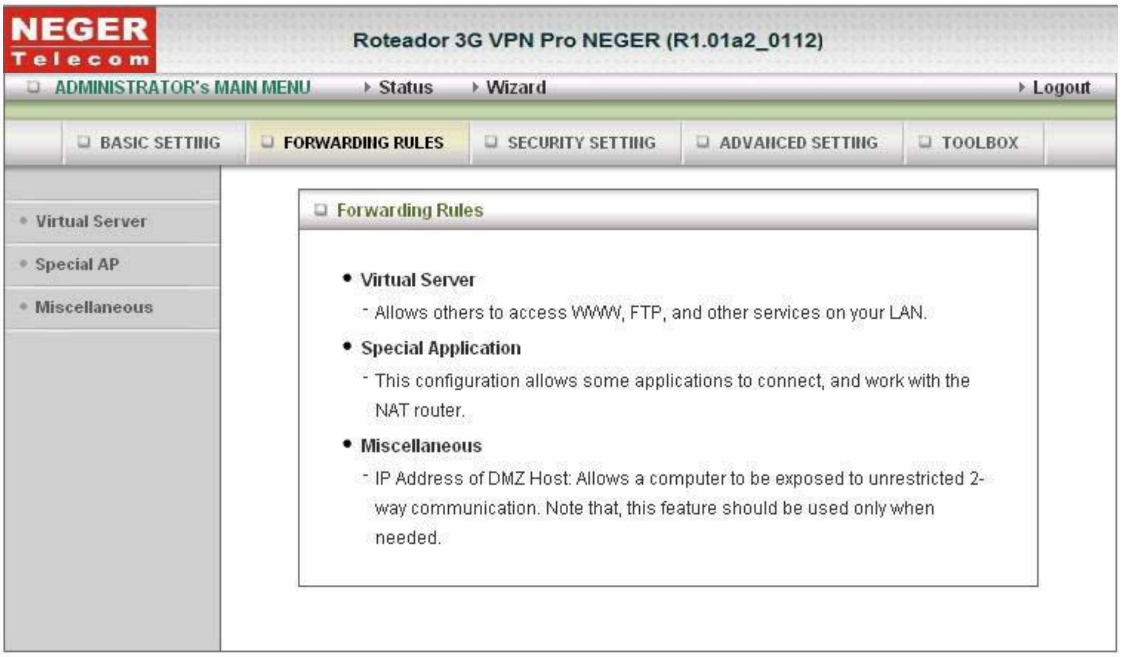
Change Password

Item	Setting
Old Password	
New Password	
Reconfirm	

You can change Password here. We **strongly** recommend you to change the system password for security reason.

Click on "Save" to store what you just select or "Undo" to give up

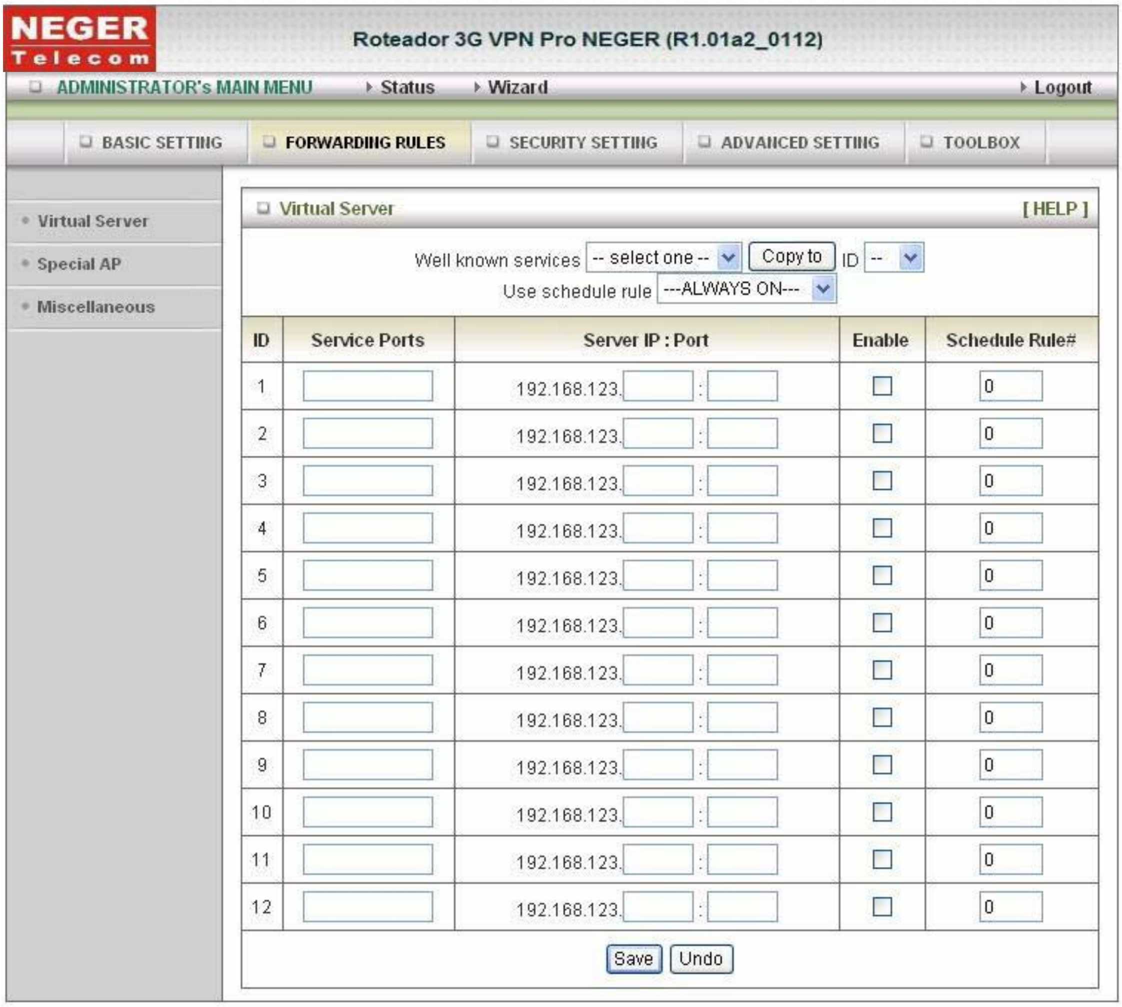
3.2.2 Forwarding Rules



Forwarding Rules

- Virtual Server
  - Allows others to access WWW, FTP, and other services on your LAN.
- Special Application
  - This configuration allows some applications to connect, and work with the NAT router.
- Miscellaneous
  - IP Address of DMZ Host: Allows a computer to be exposed to unrestricted 2-way communication. Note that, this feature should be used only when needed.

3.2.2.1 Virtual Server



Well known services -- select one -- ID --

Use schedule rule ---ALWAYS ON---

ID	Service Ports	Server IP : Port	Enable	Schedule Rule#
1		192.168.123. :	□	0
2		192.168.123. :	□	0
3		192.168.123. :	□	0
4		192.168.123. :	□	0
5		192.168.123. :	□	0
6		192.168.123. :	□	0
7		192.168.123. :	□	0
8		192.168.123. :	□	0
9		192.168.123. :	□	0
10		192.168.123. :	□	0
11		192.168.123. :	□	0
12		192.168.123. :	□	0

This product's NAT firewall filters out unrecognized packets to protect your Intranet, so all hosts behind this product are invisible to the outside world. If you wish, you can make some of them accessible by enabling the Virtual Server Mapping.

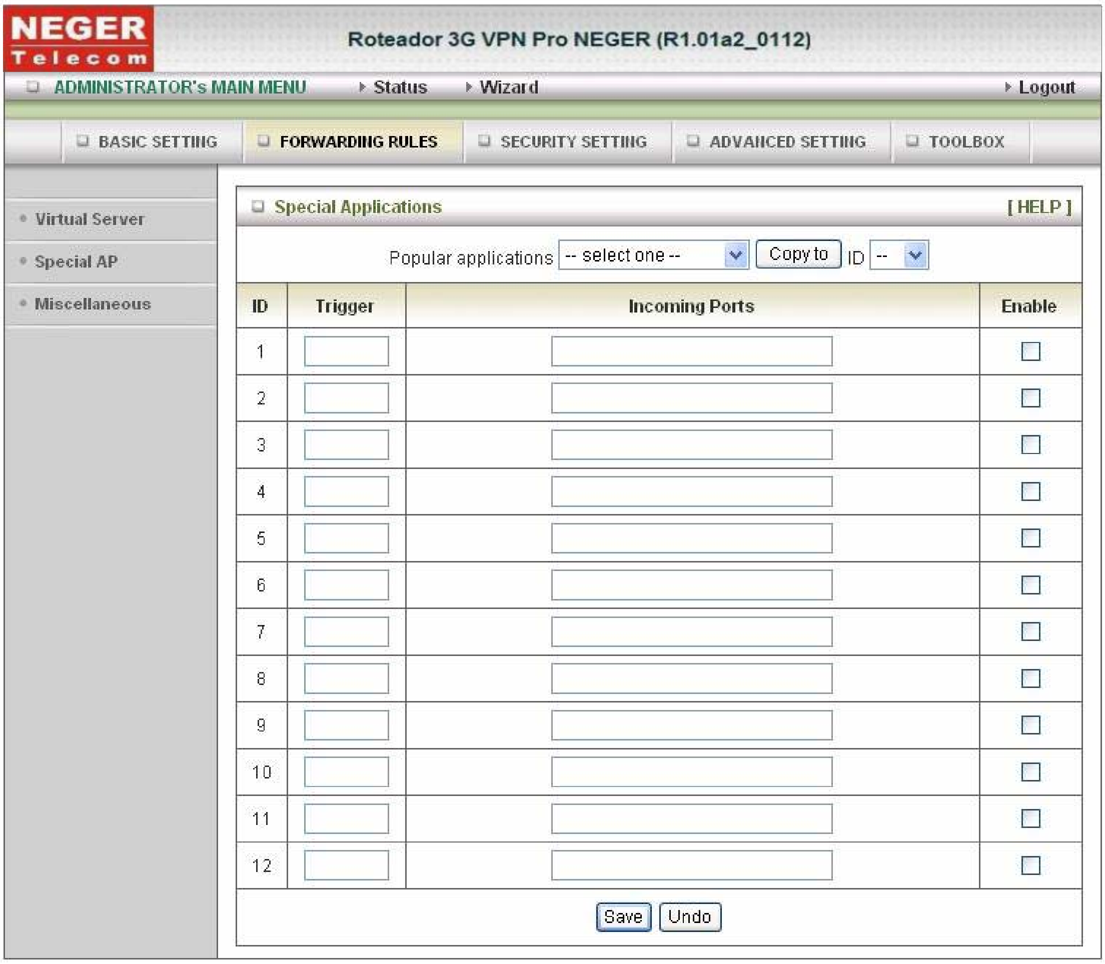
A virtual server is defined as a Service Port, and all requests to this port will be redirected to the computer specified by the Server IP. Virtual Server can work with Scheduling Rules, and give user more flexibility on Access control. For Detail, please refer to Scheduling Rule.

For example, if you have an FTP server (port 21) at 192.168.123.1, a Web server (port 80) at 192.168.123.2, and a VPN server at 192.168.123.6, then you need to specify the following virtual server mapping table:

Service Port	Server IP	Enable
21	192.168.123.1	V
80	192.168.123.2	V
1723	192.168.123.6	V

Click on "Save" to store what you just select or "Undo" to give up

3.2.2.2 Special AP



Special Applications [HELP]

Popular applications -- select one -- Copy to ID --

ID	Trigger	Incoming Ports	Enable
1			□
2			□
3			□
4			□
5			□
6			□
7			□
8			□
9			□
10			□
11			□
12			□

Some applications require multiple connections, like Internet games, Video conferencing, Internet telephony, etc. Because of the firewall function, these applications cannot work with a pure NAT router. The Special Applications feature allows some of these applications to work with this product. If the mechanism of Special Applications fails to make an application work, try setting your computer as the DMZ host instead.

1. **Trigger:** the outbound port number issued by the application.
2. **Incoming Ports**: when the trigger packet is detected, the inbound packets sent to the specified port numbers are allowed to pass through the firewall.

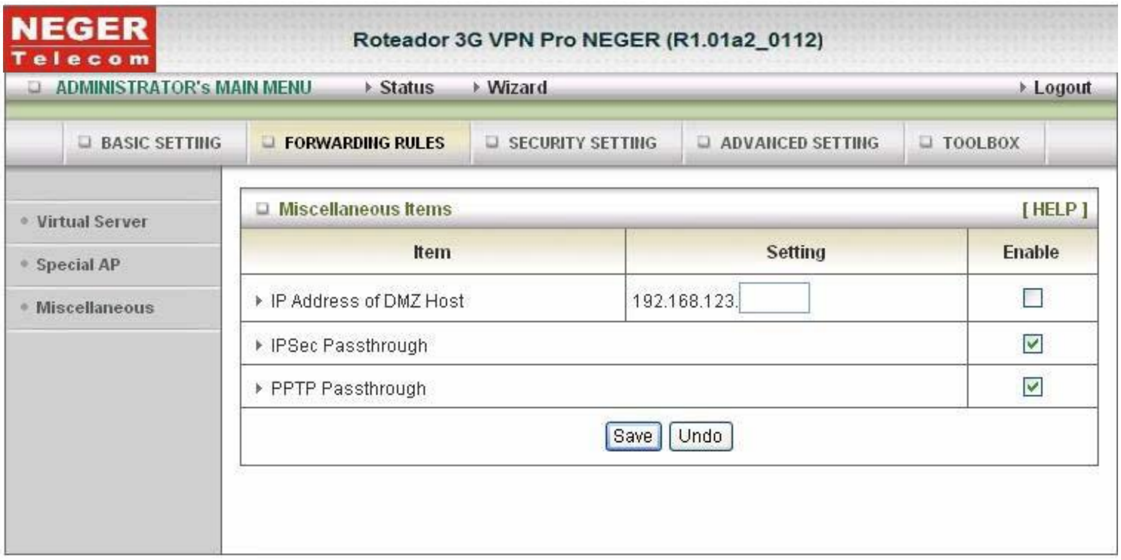
This product provides some predefined settings.

1. Select your application and
2. Click “**Copy to”** to add the predefined setting to your list.

Note! At any given time, only one PC can use each Special Application tunnel.

Click on “Save” to store what you just select or” Undo” to give up

3.2.2.3 Miscellaneous

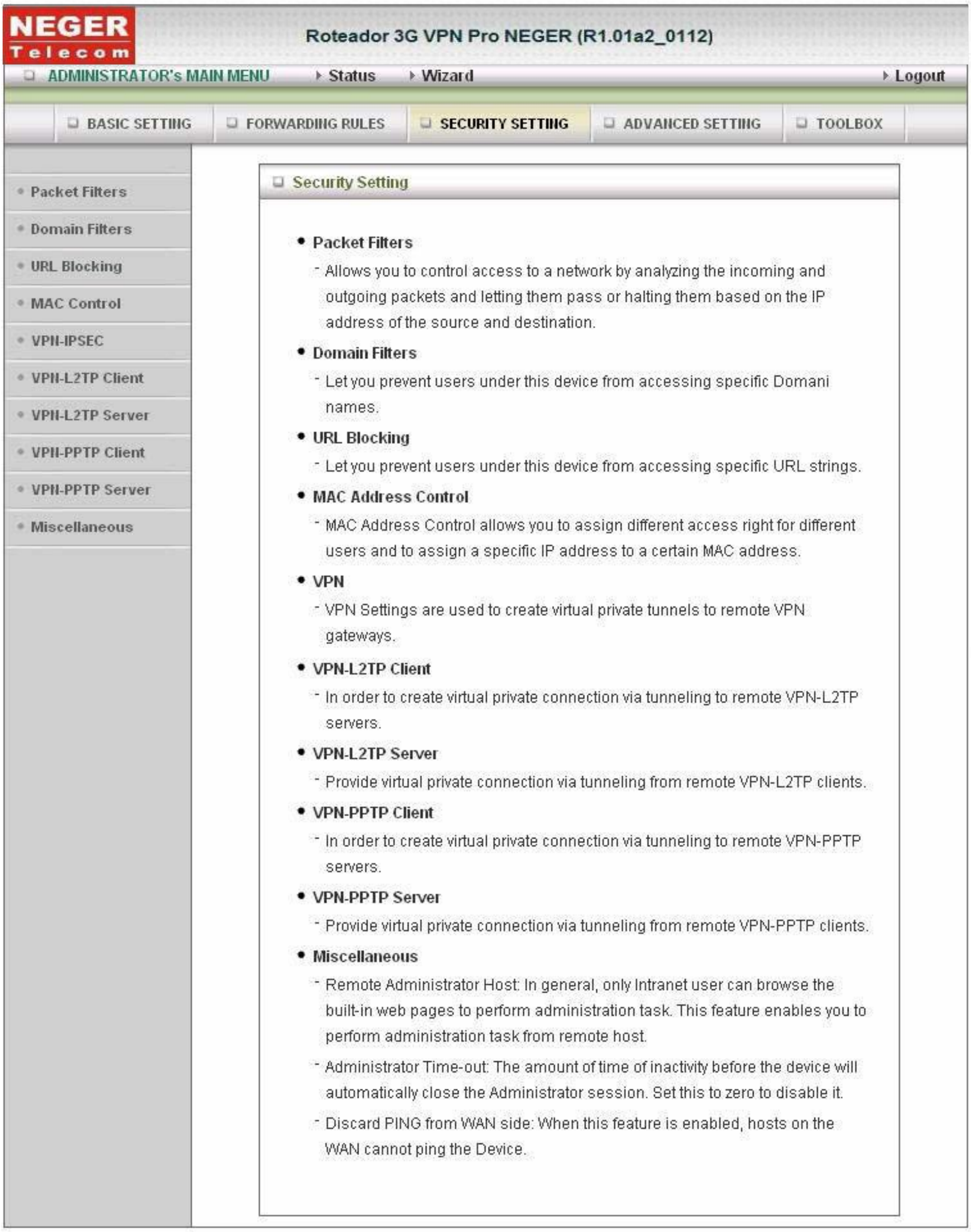


Item	Setting	Enable
IP Address of DMZ Host	192.168.123.	□
IPSec Passthrough		☑
PPTP Passthrough		☑

1. **IP Address of DMZ Host**
   DMZ (Demilitarized Zone) Host is a host without the protection of firewall. It allows a computer to be exposed to unrestricted 2-way communication for Internet games, Video conferencing, Internet telephony and other special applications.
2. **IPSec / PPTP Passthrough**
   The device also supports IPSec/PPTP Pass-through. Once VPN pass-through is enabled, multiple VPN connections can be made through the device. This is useful when you have many VPN clients on the LAN.

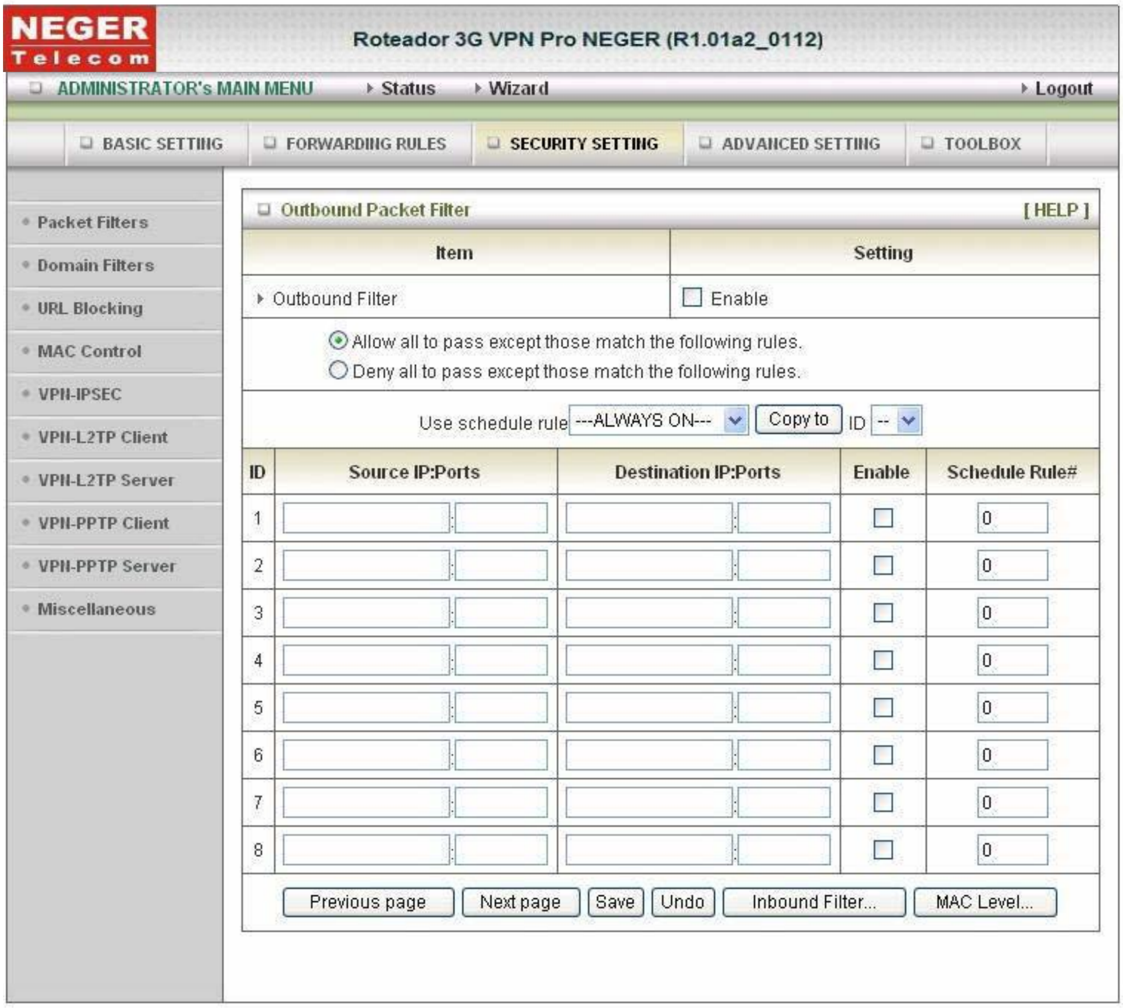
Click on “Save” to store what you just select or “Undo” to give up

3.2.3 Security Setting



- **Packet Filters**
  - Allows you to control access to a network by analyzing the incoming and outgoing packets and letting them pass or halting them based on the IP address of the source and destination.
- **Domain Filters**
  - Let you prevent users under this device from accessing specific Domani names.
- **URL Blocking**
  - Let you prevent users under this device from accessing specific URL strings.
- **MAC Address Control**
  - MAC Address Control allows you to assign different access right for different users and to assign a specific IP address to a certain MAC address.
- **VPN**
  - VPN Settings are used to create virtual private tunnels to remote VPN gateways.
- **VPN-L2TP Client**
  - In order to create virtual private connection via tunneling to remote VPN-L2TP servers.
- **VPN-L2TP Server**
  - Provide virtual private connection via tunneling from remote VPN-L2TP clients.
- **VPN-PPTP Client**
  - In order to create virtual private connection via tunneling to remote VPN-PPTP servers.
- **VPN-PPTP Server**
  - Provide virtual private connection via tunneling from remote VPN-PPTP clients.
- **Miscellaneous**
  - Remote Administrator Host: In general, only Intranet user can browse the built-in web pages to perform administration task. This feature enables you to perform administration task from remote host.
  - Administrator Time-out: The amount of time of inactivity before the device will automatically close the Administrator session. Set this to zero to disable it.
  - Discard PING from WAN side: When this feature is enabled, hosts on the WAN cannot ping the Device.

3.2.3.1 Packet Filters



Outbound Packet Filter [HELP]

Item	Setting
Outbound Filter	□ Enable

● Allow all to pass except those match the following rules.
○ Deny all to pass except those match the following rules.

Use schedule rule ---ALWAYS ON--- Copy to ID --

ID	Source IP:Ports	Destination IP:Ports	Enable	Schedule Rule#
1	:	:	□	0
2	:	:	□	0
3	:	:	□	0
4	:	:	□	0
5	:	:	□	0
6	:	:	□	0
7	:	:	□	0
8	:	:	□	0

Packet Filter includes both outbound filter and inbound filter. And they have same way to setting. Packet Filter enables you to control what packets are allowed to pass the router. Outbound filter applies on all outbound packets. However, inbound filter applies on packets that destined to Virtual Servers or DMZ host only. You can select one of the two filtering policies:

1. Allow all to pass except those match the specified rules
2. Deny all to pass except those match the specified rules

You can specify 8 rules for each direction: inbound or outbound. For each rule, you can define the following:

- Source IP address
- Source port
- Destination IP address
- Destination port
- Protocol: TCP or UDP or both.
- Use Rule#

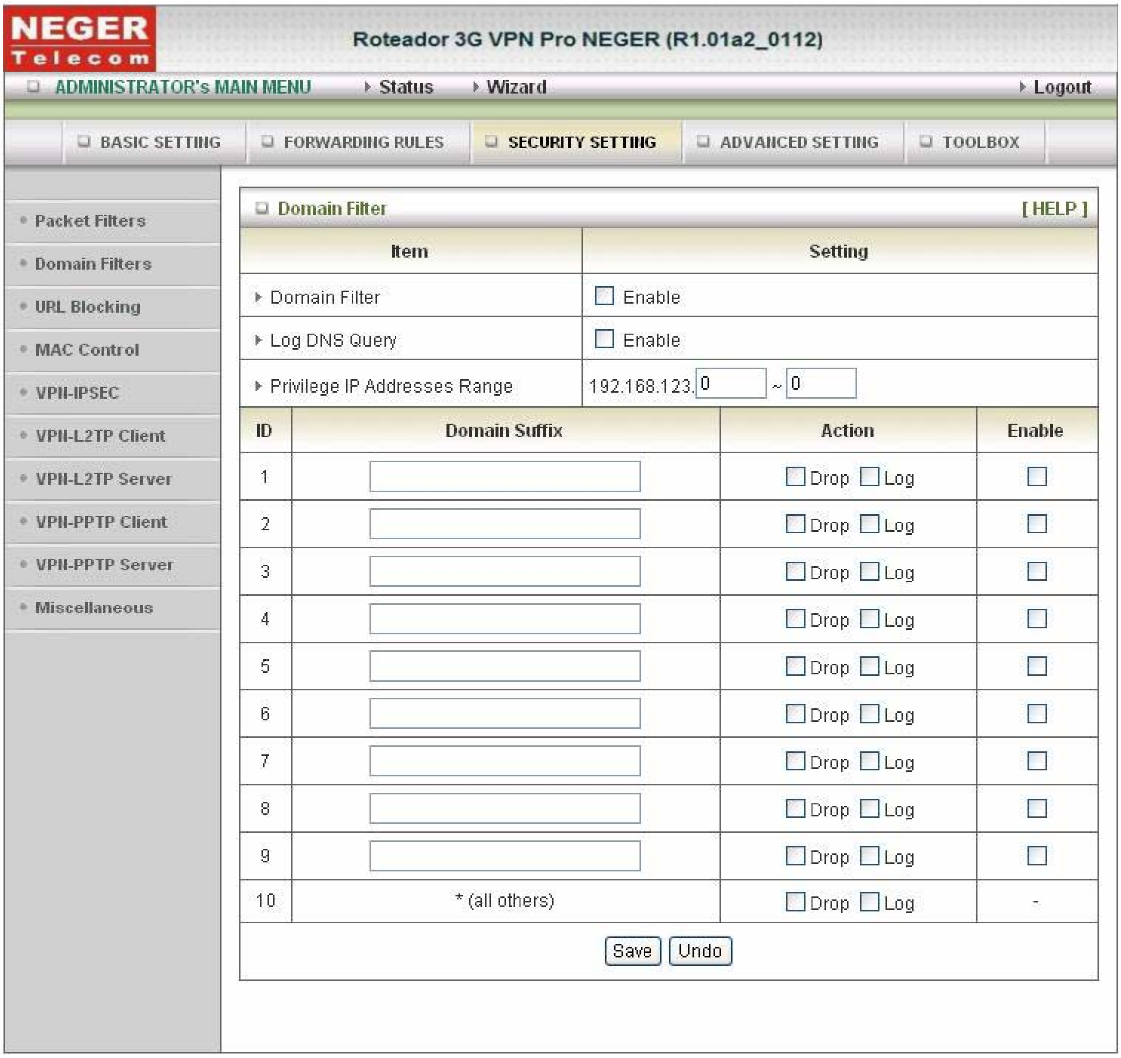
For source or destination IP address, you can define a single IP address (4.3.2.1) or a range of IP addresses

(4.3.2.1-4.3.2.254). An empty implies all IP addresses.
For source or destination port, you can define a single port (80) or a range of ports (1000-1999). Add prefix "T" or "U" to specify TCP or UDP protocol. For example, T80, U53, U2000-2999, No prefix indicates both TCP and UDP are defined. An empty implies all port addresses. Packet Filter can work with Scheduling Rules, and give user more flexibility on Access control. For Detail, please refer to Scheduling Rule.

Each rule can be enabled or disabled individually.

Click on “Save” to store what you just select or “Undo” to give up

3.2.3.2 Domain Filters



Domain Filter

Item	Setting
Domain Filter	□ Enable
Log DNS Query	□ Enable
Privilege IP Addresses Range	192.168.123. 0 ~ 0

ID	Domain Suffix	Action	Enable
1		□ Drop □ Log	□
2		□ Drop □ Log	□
3		□ Drop □ Log	□
4		□ Drop □ Log	□
5		□ Drop □ Log	□
6		□ Drop □ Log	□
7		□ Drop □ Log	□
8		□ Drop □ Log	□
9		□ Drop □ Log	□
10	* (all others)	□ Drop □ Log	-

Let you prevent users under this device from accessing specific URLs.

1. **Domain Filter Enable**

   Check if you want to enable Domain Filter.

2. **Log DNS Query**

   Check if you want to log the action when someone accesses the specific URLs.

3. **Privilege IP Address Range**

   Setting a group of hosts and privilege these hosts to access network without restriction.

4. **Domain Suffix**

   A suffix of URL can be restricted, for example, ".com", "xxx.com".

5. **Action**

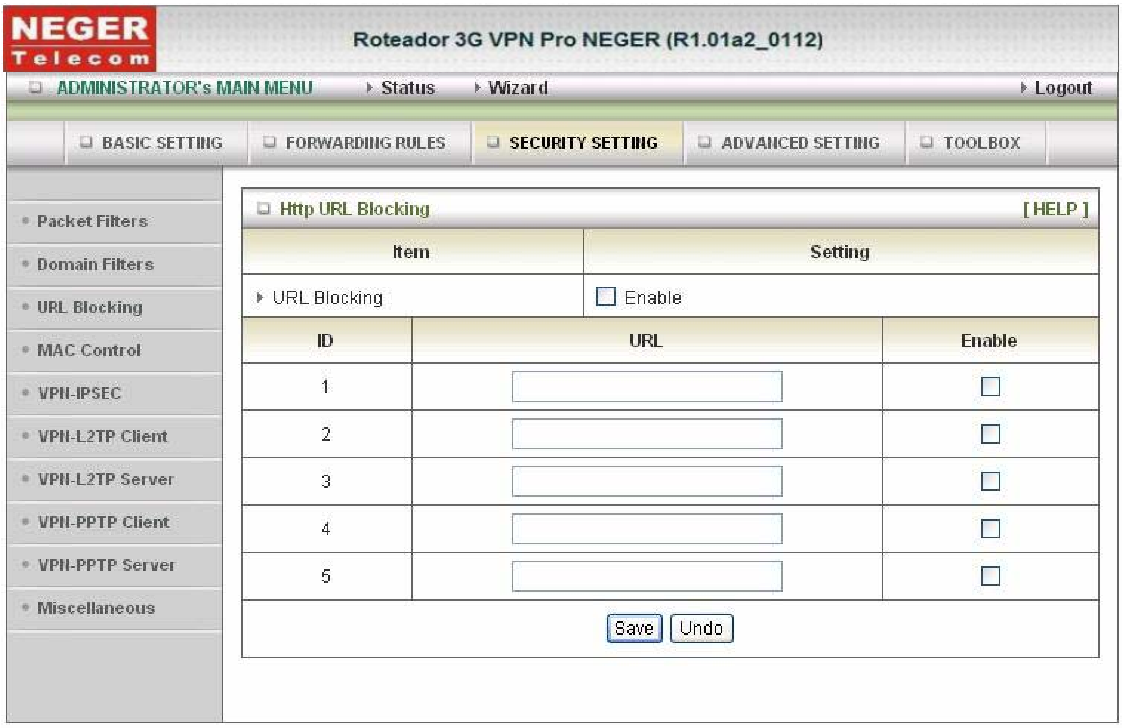
   When someone is accessing the URL met the domain-suffix, what kind of action you want. Check drop to block the access. Check “log” to log these access.

6. **Enable**

   Check to enable each rule.

Click on “Save” to store what you just select or “Undo” to give up

3.2.3.3 URL Blocking



Item	Setting
URL Blocking	□ Enable

ID	URL	Enable
1		□
2		□
3		□
4		□
5		□

URL Blocking will block LAN computers to connect to pre-define Websites. The major difference between “Domain filter” and “URL Blocking” is Domain filter require user to input suffix (like .com or .org, etc), while URL Blocking require user to input a keyword only. In other words, Domain filter can block specific website, while URL Blocking can block hundreds of websites by simply a keyword.

1. **URL Blocking Enable**

   Check if you want to enable URL Blocking.

2. **URL**

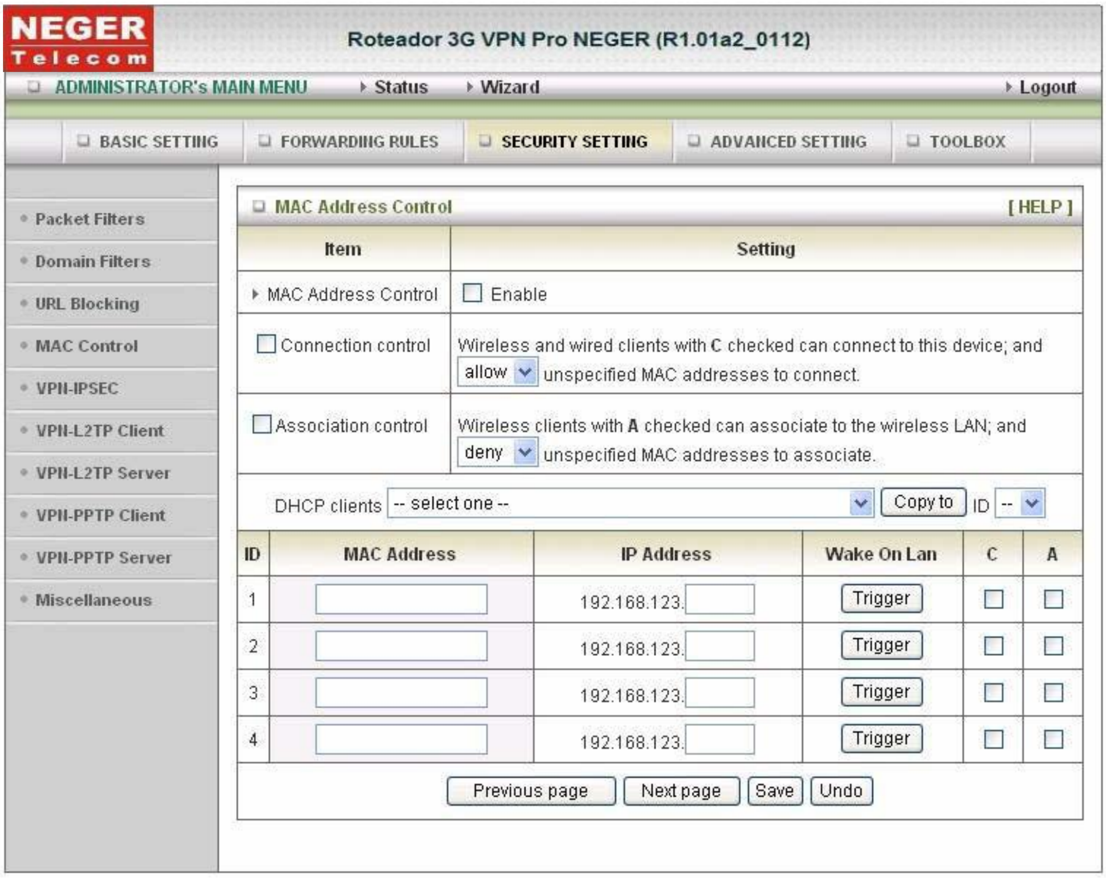
   If any part of the Website's URL matches the pre-defined word, the connection will be blocked. For example, you can use pre-defined word "sex" to block all websites if their URLs contain pre-defined word "sex".

3. **Enable**

   Check to enable each rule.

Click on “Save” to store what you just select or “Undo” to give up

3.2.3.4 MAC Address Control



MAC Address Control

Item	Setting
MAC Address Control	□ Enable
□ Connection control	Wireless and wired clients with **C** checked can connect to this device; and allow unspecified MAC addresses to connect.
□ Association control	Wireless clients with **A** checked can associate to the wireless LAN; and deny unspecified MAC addresses to associate.

DHCP clients -- select one -- Copy to ID --

ID	MAC Address	IP Address	Wake On Lan	C	A
1		192.168.123.	Trigger	□	□
2		192.168.123.	Trigger	□	□
3		192.168.123.	Trigger	□	□
4		192.168.123.	Trigger	□	□

MAC Address Control allows you to assign different access right for different users and to assign a specific IP address to a certain MAC address.

1. **MAC Address Control**

   Check “Enable” to enable the “MAC Address Control”. All of the settings in this page will take effect only when “Enable” is checked.

2. **Connection control**

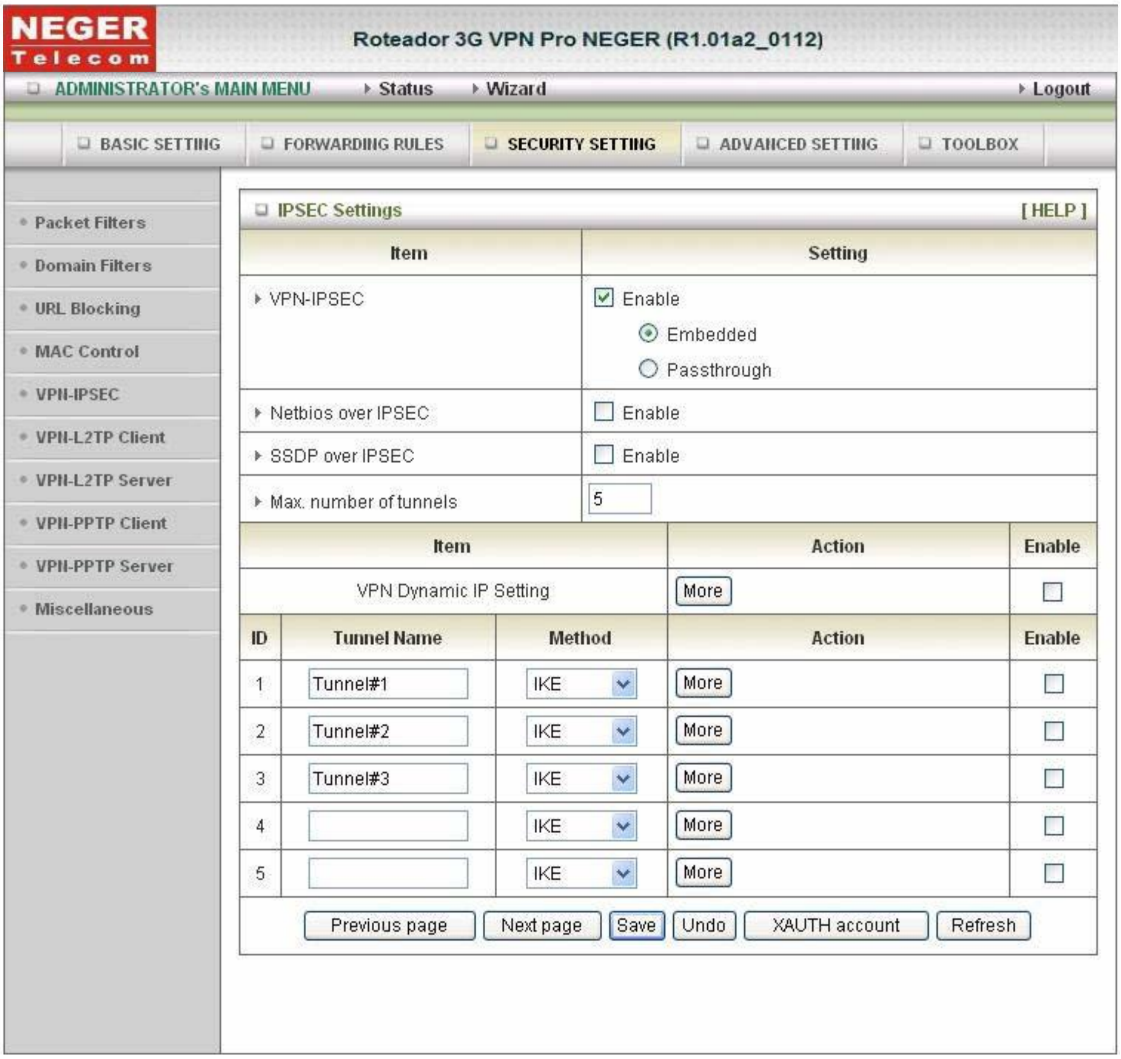
   Check "Connection control" to enable the controlling of which wired and wireless clients can connect to this device. If a client is denied to connect to this device, it means the client can't access to the Internet either. Choose "allow" or "deny" to allow or deny the clients, whose MAC addresses are not in the "Control table" (please see below), to connect to this device.

3. **Association control**

   Check "Association control" to enable the controlling of which wireless client can associate to the wireless LAN. If a client is denied to associate to the wireless LAN, it means the client can't send or receive any data via this device. Choose "allow" or "deny" to allow or deny the clients, whose MAC addresses are not in the "Control table", to associate to the wireless LAN

Click on “Save” to store what you just select or “Undo” to give up
Click on “Next Page” to go down or “Previous page” back to last page

3.2.3.5 VPN-IPSEC



Item	Setting
VPN-IPSEC	☑ Enable ● Embedded ○ Passthrough
Netbios over IPSEC	□ Enable
SSDP over IPSEC	□ Enable
Max. number of tunnels	5

Item	Action	Enable
VPN Dynamic IP Setting	More	□

ID	Tunnel Name	Method	Action	Enable
1	Tunnel#1	IKE	More	□
2	Tunnel#2	IKE	More	□
3	Tunnel#3	IKE	More	□
4		IKE	More	□
5		IKE	More	□

VPN Settings are settings that are used to create virtual private tunnels to remote VPN gateways. The tunnel technology supports data confidentiality, data origin authentication and data integrity of network information by utilizing encapsulation protocols, encryption algorithms, and hashing algorithms.

VPN-IPSEC: VPN protects network information from ill network inspectors. But it greatly degrades network throughput. Enable it when you really need a security tunnel. It is disabled for default. There are two options, Embedded VPN service or just Passthrough.

Netbios over IPSEC: Computers running Microsoft Windows can communicate with one another using NetBIOS. Users can access remote network resources by browsing the Window Network Neighborhood.

SSDP over IPSEC: Computers running Microsoft Windows can communicate with one another using SSDP on the remote IPSEC network.

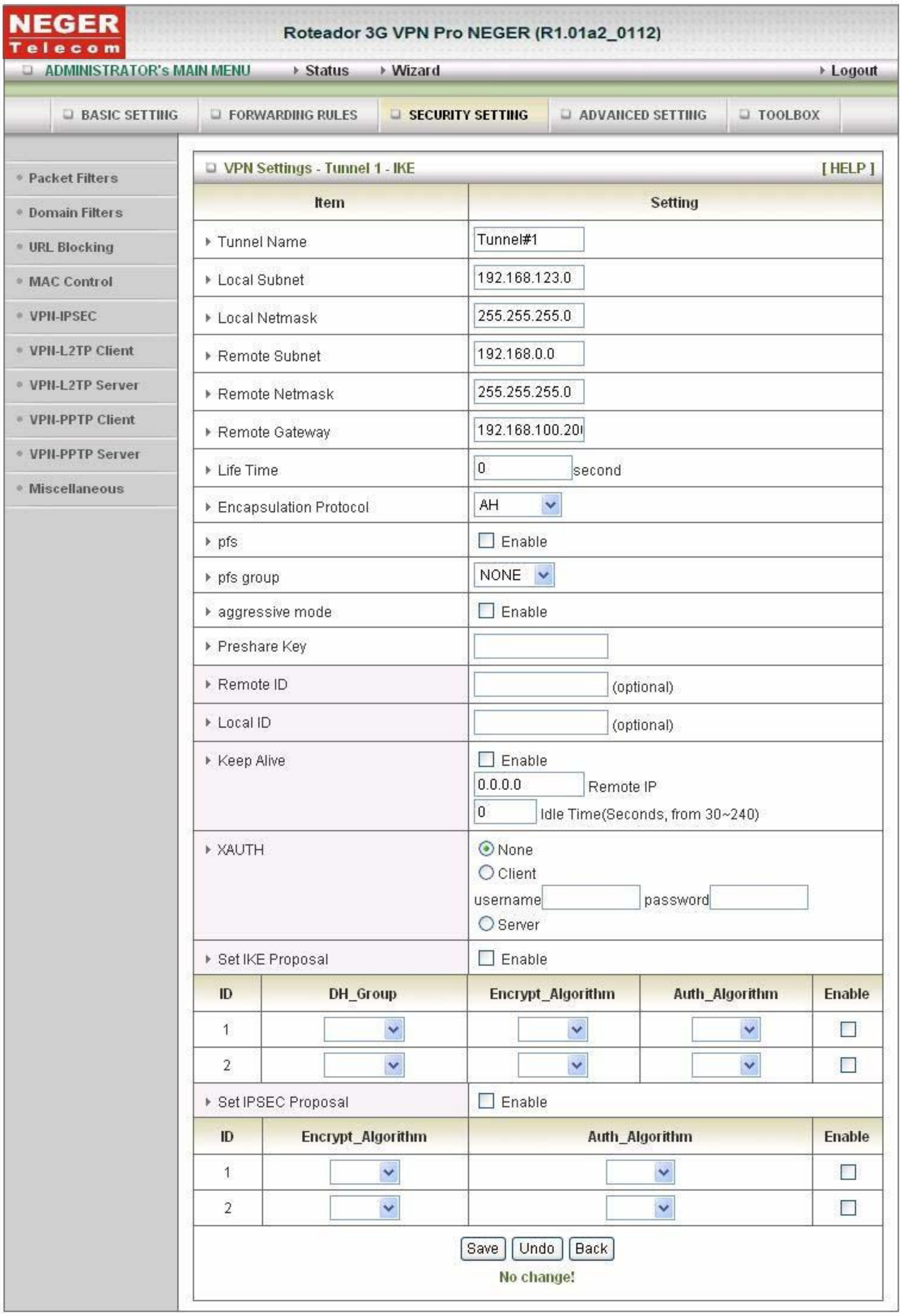
Max. number of tunnels item: Since VPN greatly degrades network throughput, the allowable maximum number of tunnels is limited. Be careful to set the value for allowing the number of tunnels can be created simultaneously. Its value ranges from 1 to 5.

Dynamic VPN settings: Enable it when you need remote mobile hosts build security tunnel with the Gateway. It is disabled for default. Click “More” button to finish detailer configuration.

Tunnel name: Indicate which tunnel that is focused now.
Method: IPSec VPN supports two kinds of key-obtained methods: manual key and automatic key exchange. Manual key approach indicates that two end VPN gateways setup authenticator and encryption key by system managers manually. However, IKE approach will perform automatic Internet key exchange. System managers of both end gateways only need set the same pre-shared key.
More...: To setup detailer configuration for manual key or IKE approaches by clicking the "More" button.

Click on “Save” to store what you just select or” Undo” to give up

VPN Settings - IKE



VPN Settings - Tunnel 1 - IKE

Item	Setting
Tunnel Name	Tunnel#1
Local Subnet	192.168.123.0
Local Netmask	255.255.255.0
Remote Subnet	192.168.0.0
Remote Netmask	255.255.255.0
Remote Gateway	192.168.100.20
Life Time	0 second
Encapsulation Protocol	AH
pfs	□ Enable
pfs group	NONE
aggressive mode	□ Enable
Preshare Key	
Remote ID	(optional)
Local ID	(optional)
Keep Alive	□ Enable 0.0.0.0 Remote IP 0 Idle Time(Seconds, from 30~240)
XAUTH	● None ○ Client username password ○ Server
Set IKE Proposal	□ Enable

ID	DH_Group	Encrypt_Algorithm	Auth_Algorithm	Enable
1				□
2				□

Set IPSEC Proposal □ Enable

ID	Encrypt_Algorithm	Auth_Algorithm	Enable
1			□
2			□

No change!

There are three parts that are necessary to setup the configuration of IKE for the dedicated tunnel: Basic setup, IKE proposal setup, and IPSec proposal setup.

Basic setup includes the setting of following items: local subnet, local netmask, remote subnet,

remote netmask, remote gateway, and pre-shared key. The tunnel name is derived from previous page of VPN setting.
IKE proposal setup includes the setting of a set of frequent-used IKE proposals and the selecting from the set of IKE proposals.
Similarly, IPSec proposal setup includes the setting of a set of frequent-used IPSec proposals and the selecting from the set of IPSec proposals.

Basic setup:

Tunnel name: Indicate which tunnel that is focused now

Local subnet: The subnet of LAN site of local VPN gateway. It can be a host, a partial subnet, and the whole subnet of LAN site of local gateway.

Local netmask: Local netmask combined with local subnet to form a subnet domain.

Remote subnet: The subnet of LAN site of remote VPN gateway, it can be a host, a partial subnet, and the whole subnet of LAN site of remote gateway.

Remote netmas: Remote netmask combined with remote subnet to form a subnet domain of remote end.

Remote gateway: The IP address of remote VPN gateway.

Life time: The unit of life time is based on the value of Life Time Unit. The value of unit is second, the value of life time represents the life time of dedicated VPN tunnel between both end gateways. Its value ranges from 300 seconds to 172,800 seconds.

Encapsulation protocol: There are two protocols can be selected: ESP and AH.

pfs: Configures perfect forward secrecy for connections created with this IPSec transport profile by assigning a Diffie-Hellman prime modulus group.

pfs Group: There are three groups can be selected: , None, Group 1, Group 2, Group 5.
None: No pfs group
Group 1: 768-bit Diffie-Hellman prime modulus group
Group 2: 1024-bit Diffie-Hellman prime modulus group
Group 5: 1536-bit Diffie-Hellman prime modulus group

Aggressive Mode: Enabling this mode will accelerate establishing tunnel, but the devicewill suffer from less security in the meanwhile. Hosts in both ends of the tunnel must support this mode so as to establish the tunnel properly.

Pre-shared key: The first key that supports IKE mechanism of both VPN gateways for negotiating further security keys. The pre-shared key must be same for both end gateways.

Remote ID: The Type and the Value are must same as the Type and the Value of the Local ID of the remote VPN gateway.

Local ID: The Type and the Value are must same as the Type and the Value of the Remote ID of the remote VPN gateway.

IKE Keep Alive(Ping IP Address): Input the IP address of remote host that exist in the opposite side of the VPN tunnel (Ex. You can input the LAN IP address of remote VPN gateway). The device will start to Ping remote host when there is no traffic within the VPN tunnel. If the device can't get ICMP response from remote host anymore, then it will terminate the VPN tunnel automatically.

Extended Authentication (xAuth): With xAuth feature, the VPN client (or initiator) needs to provide additional user information to remote VPN server (or VPN gateway) for extended authentication. The VPN server would reject the connect request from VPN clients because of the unknown user, even though the pre-shared key is correct. This function is suitable to remote mobile VPN clients. You can not only configure a VPN rule with a pre-shared key for all remote users using, but you can also designate only someone is permitted to establish VPN connection with VPN server.
xAuth - None: Without Extended Authentication(xAuth).
xAuth -Server mode: Check this checkbox if the device behaves as a VPN server, and will verify the legality of user information from VPN client. The user information that is provided by VPN client needs to match to user information that is in local user database of VPN server. You can press "Set local user" button to edit local user database. Please note that only VPN clients with xAuth can establish VPN connection with the device if you have checked this checkbox.
xAuth - Client mode: Check this checkbox if the device behaves as a VPN server, and will send user information to remote VPN server for extended authentication. You need to input correct user name and password to pass authentication. Please note that remote VPN server which is without xAuth will reject your connect request if you have checkedthis checkbox.
xAuth-User Name: Input user name that is provided by remote VPN server. This field is for xAUTH client mode use only.
xAuth-Password: Input password that is corresponded to the user name above. This field is for xAUTH client mode use only.

IKE proposal setup

Set IKE Proposal: Check this checkbox to enable IKE proposals. The default value will be use if this option is disabled. .

DH group: There are three groups can be selected: group 1 (MODP768), group 2 (MODP1024), group 5 (MODP1536).

Encryption algorithm: There are two algorithms can be selected: 3DES and DES.

Authentication algorithm: There are two algorithms can be selected: SHA1 and MD5.

Enable: Check this checkbox to enable the IKE Proposal with this rule.

IPSec proposal setup

Set IPSec proposal: Check this checkbox to enable IPSec proposals. The default value will be use if this option is disabled.

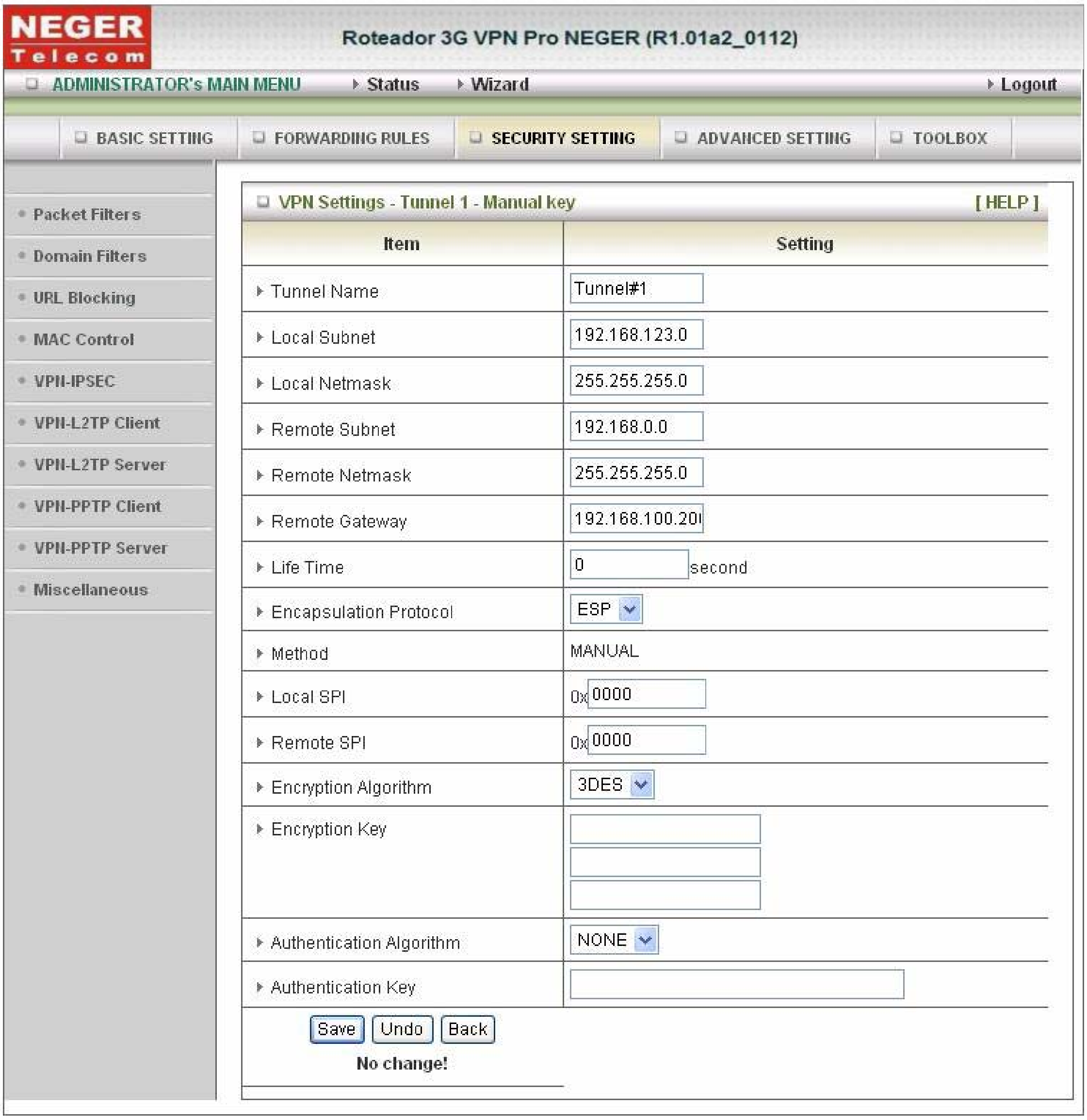
Encryption algorithm: There are two algorithms can be selected: 3DES and DES. But when the encapsulation protocol is AH, encryption algorithm is unnecessarily set.

Authentication algorithm: There are two algorithms can be selected: SHA1 and MD5. But none also can be selected here for IPSec proposal.

Enable: Check this checkbox to enable extended authentication with this rule.

Click on “Save” to store what you just select or” Undo” to give up

VPN Settings - Manual key



VPN Settings - Tunnel 1 - Manual key

Item	Setting
Tunnel Name	Tunnel#1
Local Subnet	192.168.123.0
Local Netmask	255.255.255.0
Remote Subnet	192.168.0.0
Remote Netmask	255.255.255.0
Remote Gateway	192.168.100.20
Life Time	0 second
Encapsulation Protocol	ESP
Method	MANUAL
Local SPI	0x 0000
Remote SPI	0x 0000
Encryption Algorithm	3DES
Encryption Key	
Authentication Algorithm	NONE
Authentication Key	

No change!

Tunnel name: Indicate which tunnel that is focused now.

Local Subnet: The subnet of LAN site of local VPN gateway. It can be a host, a partial subnet, or the whole subnet of LAN site of local gateway.

Local Netmask: Local netmask combined with local subnet to form a subnet domain.

Remote Subnet: The subnet of LAN site of remote VPN gateway, it can be a host, a partial subnet, or the whole subnet of LAN site of remote gateway.

Remote Netmask: Remote netmask combined with remote subnet to form a subnet domain of remote end.

Remote Gateway: The IP address of remote VPN gateway.

Life Time: The unit of life time is based on the value of Life Time Unit. The value of unit is second, the value of life time represents the life time of dedicated VPN tunnel between both end gateways. Its value ranges from 300 seconds to 172,800 seconds.

Encapsulation protocol: There are two protocols can be selected: ESP and AH.

Local SPI: SPI is an important parameter during hashing. Local SPI will be included in the outbound packet transmitted from WAN site of local gateway. The value of local SPI should be set in hex formatted.

Remote SPI: Remote SPI will be included in the inbound packet transmitted from WAN site of remote gateway. It will be used to de-hash the coming packet and check its integrity. The value of remote SPI should be set in hex formatted.

Encryption algorithm: There are two algorithms can be selected: 3DES and DES. But when the encapsulation protocol is AH, encryption algorithm is unnecessarily set.

Encryption key: Encryption key is used by the encryption algorithm. Its length is 8 bytes if encryption algorithm is DES or 24 bytes if 3DES. The key value should be set in hex formatted.

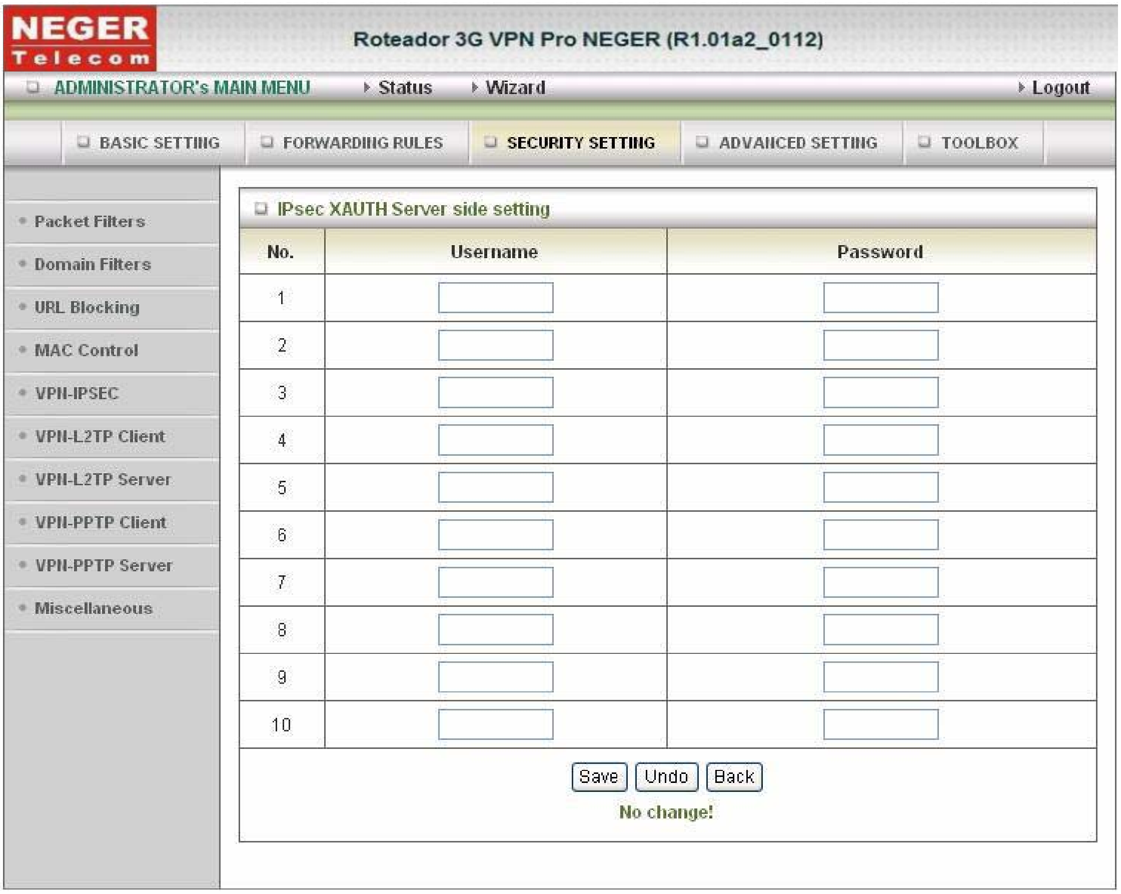
Authentication algorithm: There are two algorithms can be selected: SHA1 and MD5. But none also can be selected here for non hashing operation.

Authentication key: Authentication key is used by the authentication algorithm. Its length is 16 bytes if authentication algorithm is MD5 or 20 bytes if SHA1. Certainly, its length will be 0 if no authentication algorithm is chosen. The key value should be set in hex formatted.

Click on “Save” to store what you just select or” Undo” to give up

VPN Settings - IPsec XAuth

You can edit user information with this configuration page. This user information is for XAuth server mode use only.

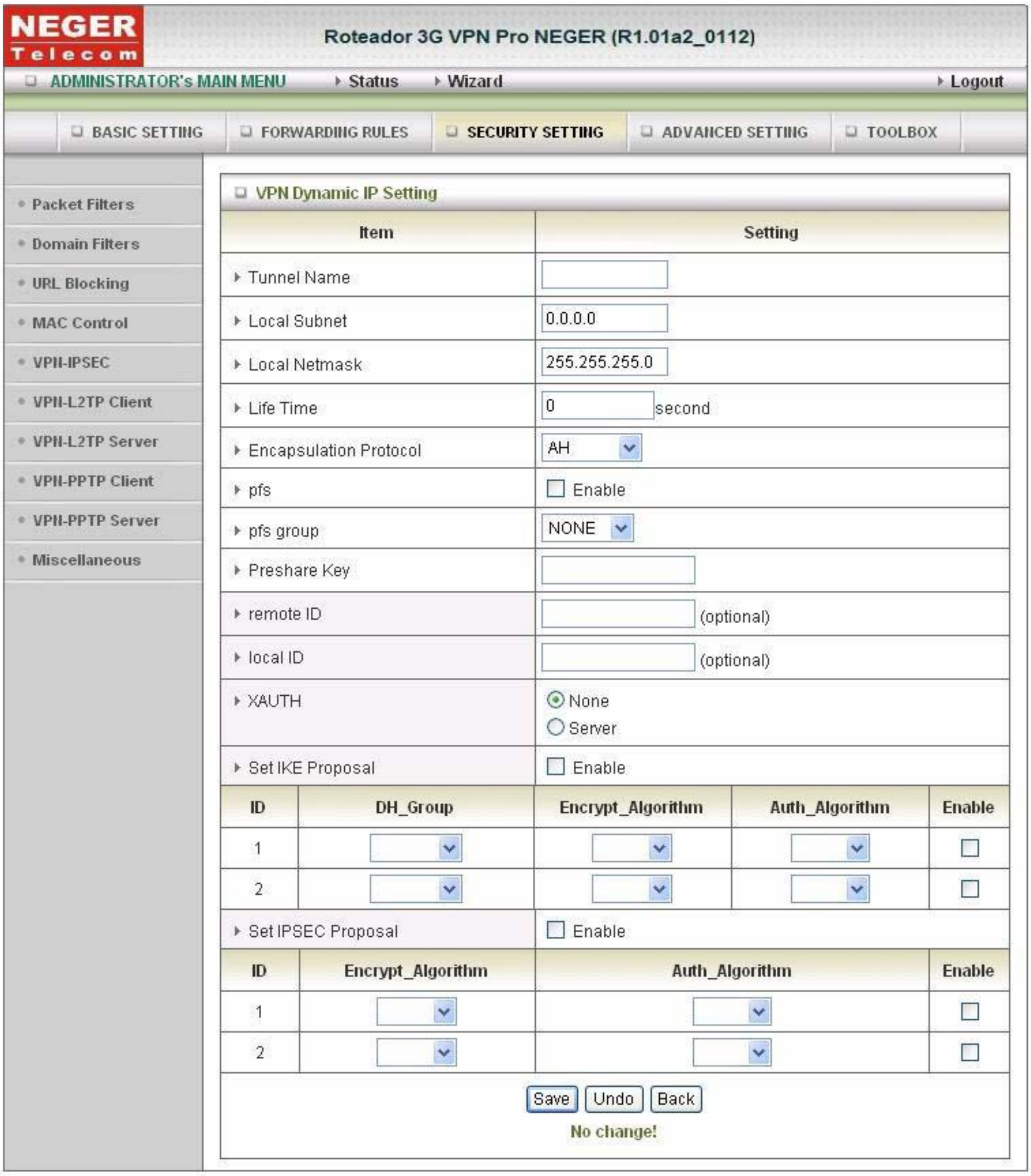


IPsec XAUTH Server side setting

No.	Username	Password
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		

No change!

VPN Settings – VPN Dynamic IP Setting



VPN Dynamic IP Setting

Item	Setting
Tunnel Name	
Local Subnet	0.0.0.0
Local Netmask	255.255.255.0
Life Time	0 second
Encapsulation Protocol	AH
pfs	□ Enable
pfs group	NONE
Preshare Key	
remote ID	(optional)
local ID	(optional)
XAUTH	● None ○ Server
Set IKE Proposal	□ Enable

ID	DH_Group	Encrypt_Algorithm	Auth_Algorithm	Enable
1				□
2				□

Set IPSEC Proposal □ Enable

ID	Encrypt_Algorithm	Auth_Algorithm	Enable
1			□
2			□

No change!

VPN gateway can ignore IP information of client when using Dynamic VPN, so it is suitable for users to build VPN tunnel with VPN gateway from remote mobile host.

Tunnel name: Indicate which tunnel that is focused now.

Local subnet: The subnet of LAN site of local VPN gateway. It can be a host, a partial subnet, and the whole subnet of LAN site of local gateway.

Local Netmask: Local netmask combined with local subnet to form a subnet domain.

Life time: The unit of life time is based on the value of Life Time Unit. The value of unit is second, the value of life time represents the life time of dedicated VPN tunnel between both end gateways. Its value ranges from 300 seconds to 172,800 seconds.

Encapsulation protocol: There are two protocols can be selected: ESP and AH.

pfs: Configures perfect forward secrecy for connections created with this IPSec transport profile by assigning a Diffie-Hellman prime modulus group.

pfs Group: There are three groups can be selected: , None, Group 1, Group 2, Group 5.
None: No pfs group
Group 1: 768-bit Diffie-Hellman prime modulus group
Group 2: 1024-bit Diffie-Hellman prime modulus group
Group 5: 1536-bit Diffie-Hellman prime modulus group

Preshared key: The first key that supports IKE mechanism of both VPN gateway and VPN client host for negotiating further security keys. The pre-shared key must be same for both VPN gateways and clients.

Remote ID: The Type and the Value are must same as the Type and the Value of the Local ID of the remote VPN gateway.

Local ID: The Type and the Value are must same as the Type and the Value of the Remote ID of the remote VPN gateway.

Extended Authentication (xAuth): With xAuth feature, the VPN client (or initiator) needs to provide additional user information to remote VPN server (or VPN gateway) for extended authentication. The VPN server would reject the connect request from VPN clients because of the unknown user, even though the pre-shared key is correct. This function is suitable to remote mobile VPN clients. You can not only configure a VPN rule with a pre-shared key for all remote users using, but you can also designate only someone is permitted to establish VPN connection with VPN server.
xAuth - None: Without Extended Authentication(xAuth).
xAuth -Server mode: Check this checkbox if the device behaves as a VPN server, and will verify the legality of user information from VPN client. The user information that is provided by VPN client needs to match to user information that is in local user database of VPN server. You can press "Set local user" button to edit local user database. Please note that only VPN clients with xAuth can establish VPN connection with the device if you have checked this checkbox.

IKE proposal setup

Set IKE Proposal: Check this checkbox to enable IKE proposals. The default value will be use if this option is disabled. .

DH group: There are three groups can be selected: group 1 (MODP768), group 2 (MODP1024), group 5 (MODP1536).

Encryption algorithm: There are two algorithms can be selected: 3DES and DES.

Authentication algorithm: There are two algorithms can be selected: SHA1 and MD5.

Enable: Check this checkbox to enable the IKE Proposal with this rule.

IPSec proposal setup

Set IPSec proposal: Check this checkbox to enable IPSec proposals. The default value will be use if this option is disabled.

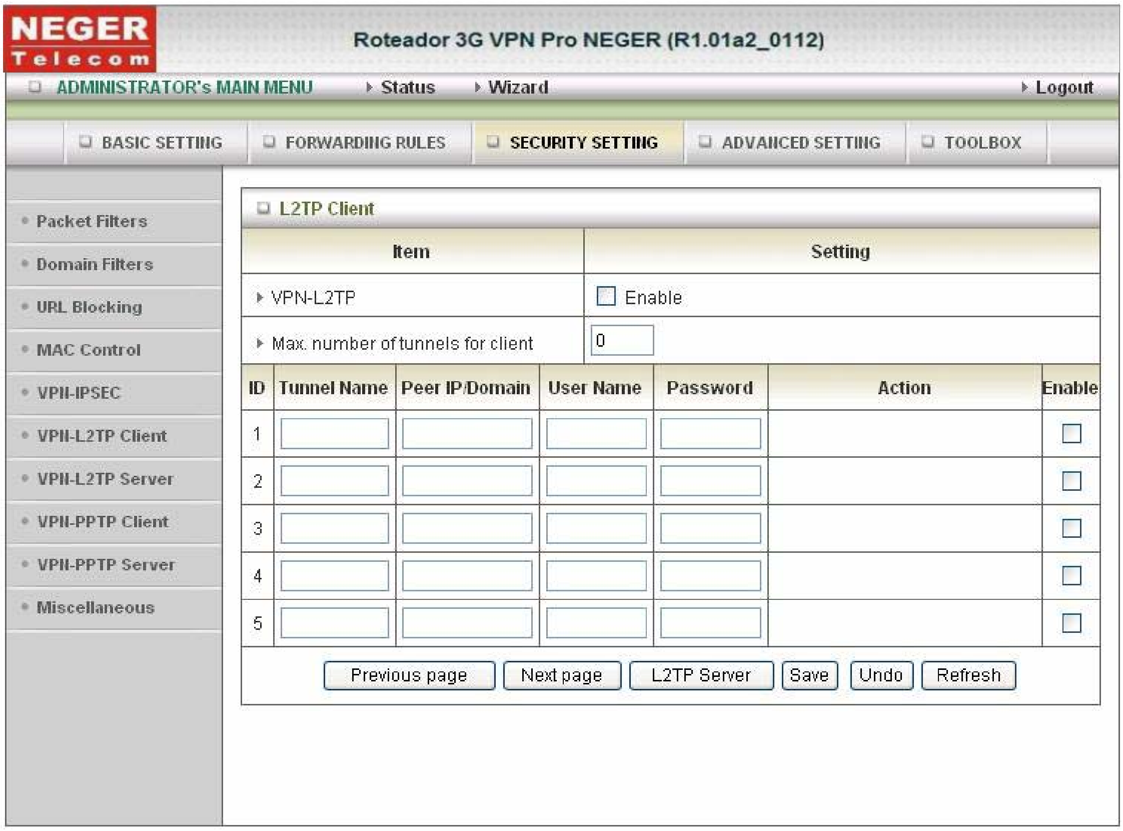
Encryption algorithm: There are two algorithms can be selected: 3DES and DES. But when the encapsulation protocol is AH, encryption algorithm is unnecessarily set.

Authentication algorithm: There are two algorithms can be selected: SHA1 and MD5. But none also can be selected here for IPSec proposal.

Enable: Check this checkbox to enable extended authentication with this rule.

Click on “Save” to store what you just select or” Undo” to give up

VPN-L2TP Client



L2TP Client

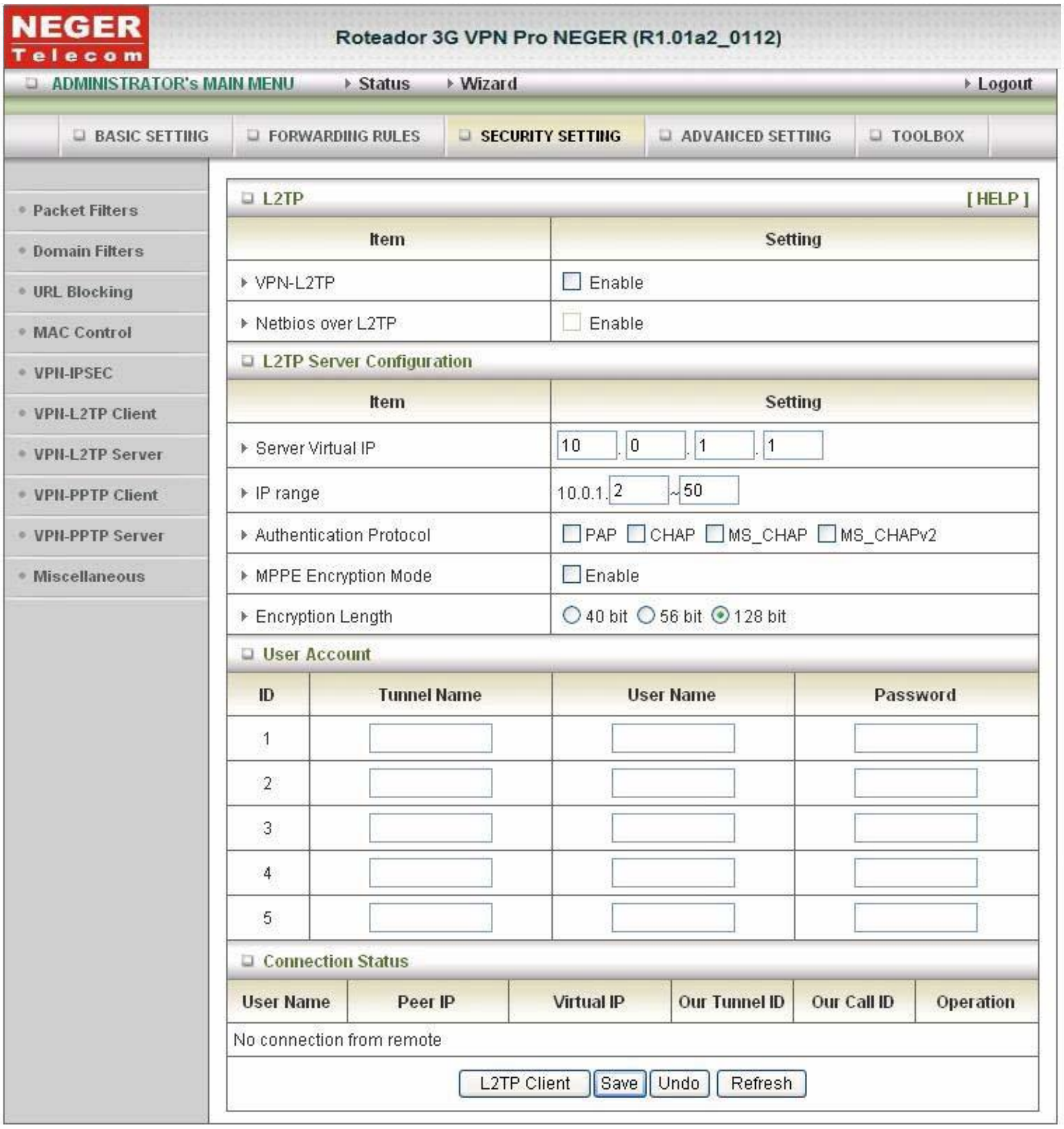
Item	Setting
VPN-L2TP	□ Enable
Max. number of tunnels for client	0

ID	Tunnel Name	Peer IP/Domain	User Name	Password	Action	Enable
1						□
2						□
3						□
4						□
5						□

1. **VPN-L2TP:** Enables or Disables the L2TP client.
2. **Max. number of tunnels client:**
3. **Tunnel Name:** The name of Item.
4. **Peer IP/Domain:** The IP/Domain of L2TP server is.
5. **L2TP Account and Password:** the account and password your ISP assigned to you. If you don't want to change the password, keep it empty.
6. **Action:** The status of this tunnel.
7. **Enable:** Check to enable each rule.

Click on "Save" to store what you just select or" Undo" to give up

3.2.3.6 VPN-L2TP Server



L2TP

Item	Setting
VPN-L2TP	□ Enable
Netbios over L2TP	□ Enable

L2TP Server Configuration

Item	Setting
Server Virtual IP	10 . 0 . 1 . 1
IP range	10.0.1. 2 ~ 50
Authentication Protocol	□ PAP □ CHAP □ MS_CHAP □ MS_CHAPv2
MPPE Encryption Mode	□ Enable
Encryption Length	○ 40 bit ○ 56 bit ● 128 bit

User Account

ID	Tunnel Name	User Name	Password
1			
2			
3			
4			
5			

Connection Status

User Name	Peer IP	Virtual IP	Our Tunnel ID	Our Call ID	Operation
No connection from remote					

The VPN gateway can behave as a L2TP server, and allows remote hosts to access LAN servers after establishing L2TP connection with it. The device can support three authentication methods: PAP, CHAP, MSCHAP(v1) and MSCHAP(v2). Users can also enable MPPE encryption when using MSCHAP.

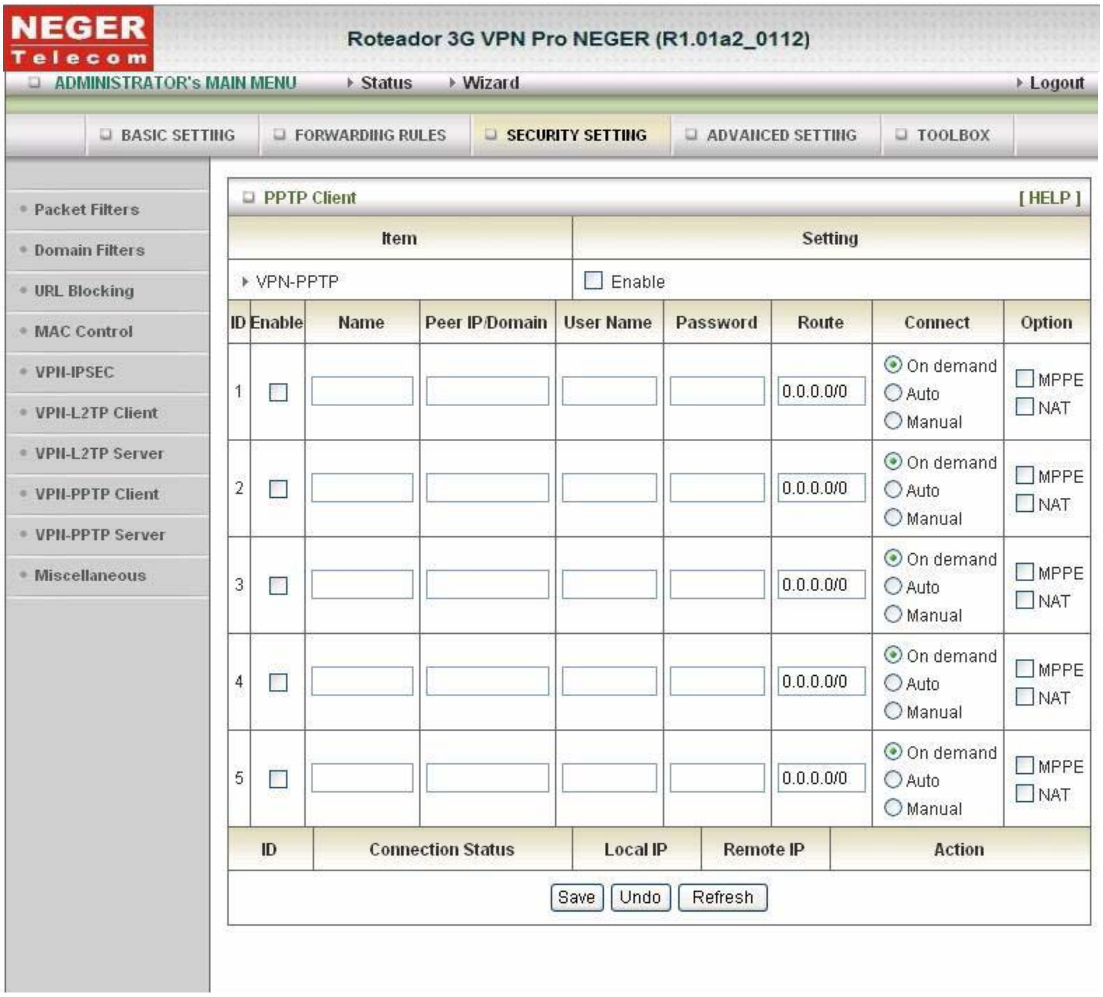
1. **Server Virtual IP:** Check this checkbox to enable function of L2TP server.
2. **Virtual IP of L2TP Server:** The IP address of L2TP server. This IP address should be different from IP address of PPTP server and LAN subnet of VPN gateway.
3. **Authentication Protocol:** Users can choose authentication protocol as PAP, CHAP, or MSCHAP(v1).
4. **MPPE Encryption Mode:** Check this checkbox to enable MPPE encryption. Please note that MPPE needs to work with MSCHAP authentication method.

User Account Setting

Users can input five different user accounts for L2TP server.
Tunnel Name: Input the name for tunnel.
User Name: Input a user name that is allowed to establish L2TP connection with VPN gateway
Password: Input the password for the user.

Click on "Save" to store what you just select or" Undo" to give up

3.2.3.7 VPN-PPTP Client



PPTP Client [HELP]

Item	Setting
VPN-PPTP	□ Enable

ID	Enable	Name	Peer IP/Domain	User Name	Password	Route	Connect	Option
1	□					0.0.0.0/0	● On demand ○ Auto ○ Manual	□ MPPE □ NAT
2	□					0.0.0.0/0	● On demand ○ Auto ○ Manual	□ MPPE □ NAT
3	□					0.0.0.0/0	● On demand ○ Auto ○ Manual	□ MPPE □ NAT
4	□					0.0.0.0/0	● On demand ○ Auto ○ Manual	□ MPPE □ NAT
5	□					0.0.0.0/0	● On demand ○ Auto ○ Manual	□ MPPE □ NAT

ID	Connection Status	Local IP	Remote IP	Action

1. **VPN-PPTP:** Enables or Disables the PPTP client.
2. **Enable:** Check to enable each rule.
3. **Name:** The name of Item.
4. **Peer IP/Domain:** The IP/Domain of PPTP server is.
5. **PPTP Account and Password:** the account and password your ISP assigned to you. I you don't want to change the password, keep it empty.
6. **Route:** Which connection will use the PPTP section?
7. **Connect**: There are 3 modes to select:

   On demand: The device will link up with ISP when the clients send outgoing packets.

   Auto: The device will link with ISP until the connection is established.

   Manually: The device will not make the link until someone clicks the connect-button in the Status-page.

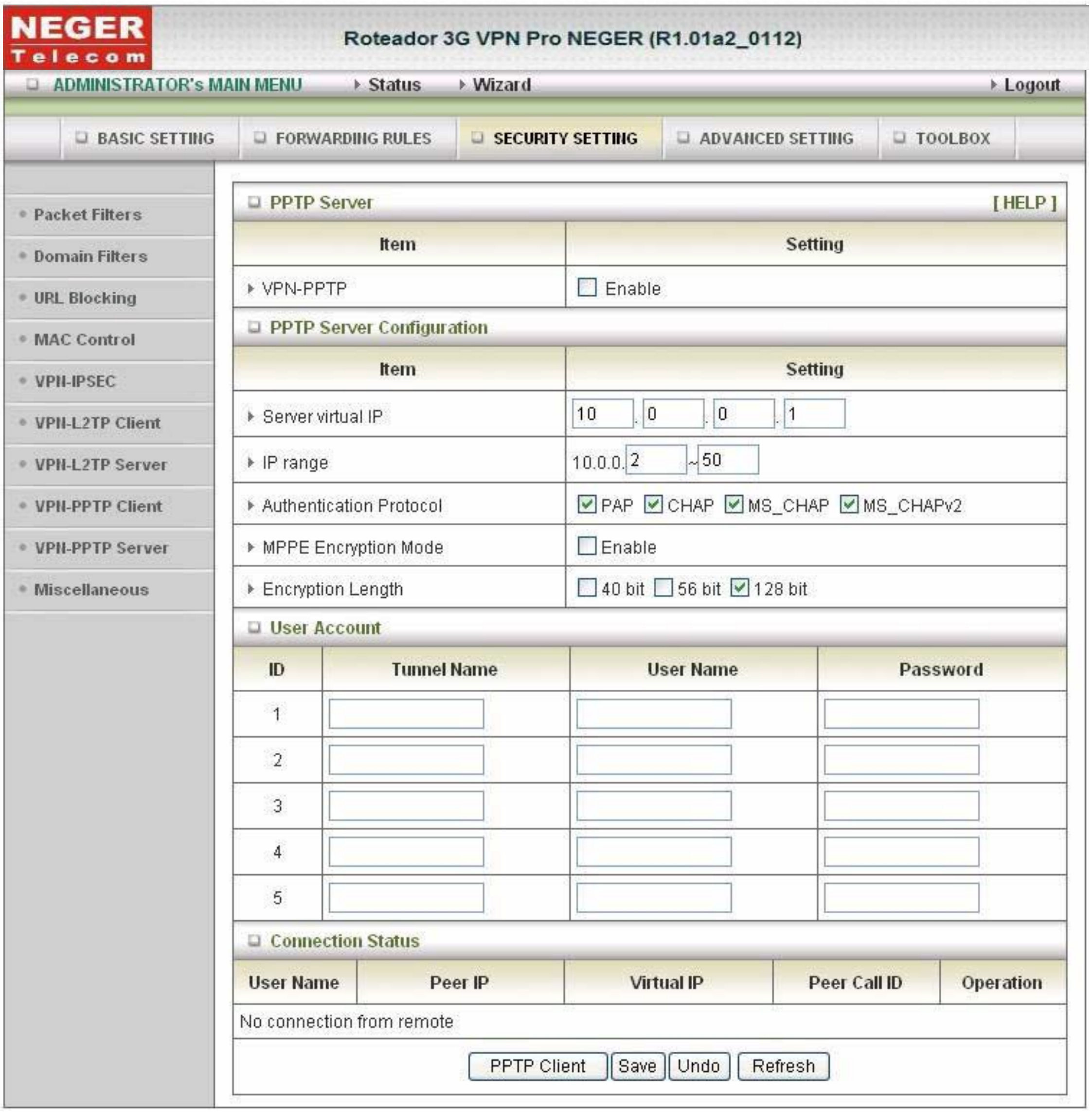
8. **Option:**

   MPPE: The MPPE encryption supports.

NAT: The Nat Traversal supports.

Click on "Save" to store what you just select or" Undo" to give up

3.2.3.8 VPN-PPTP Server



PPTP Server

Item	Setting
VPN-PPTP	□ Enable

PPTP Server Configuration

Item	Setting
Server virtual IP	10 . 0 . 0 . 1
IP range	10.0.0. 2 ~ 50
Authentication Protocol	☑ PAP ☑ CHAP ☑ MS_CHAP ☑ MS_CHAPv2
MPPE Encryption Mode	□ Enable
Encryption Length	□ 40 bit □ 56 bit ☑ 128 bit

User Account

ID	Tunnel Name	User Name	Password
1			
2			
3			
4			
5			

Connection Status

User Name	Peer IP	Virtual IP	Peer Call ID	Operation
No connection from remote				

The VPN gateway can behave as a PPTP server, and allows remote hosts to access LAN servers after establishing PPTP connection with it. The device can support three authentication methods: PAP, CHAP, MSCHAP(v1) and MSCHAP(v2). Users can also enable MPPE encryption when using MSCHAP.

1. **VPN-PPTP:** Check this checkbox to enable function of PPTP server.
2. **Server virtual IP:** The IP address of PPTP server. This IP address should be differen from
   IP address of PPTP server and LAN subnet of VPN gateway.
3. **IP range:** The client IP range. IPs in this range are given clients trying to connect.
4. **Authentication Protocol:** Users can choose authentication protocol as PAP, CHAP, or MS_CHAP(v1), MS_CHAP(v2).
5. **MPPE Encryption Mode:** Check this checkbox to enable MPPE encryption. Please note that MPPE needs to work with MSCHAP authentication method.
6. **Encryption Length:** There are 3 kind of encryption for MPPE, 40bits, 56bits and 128bits.

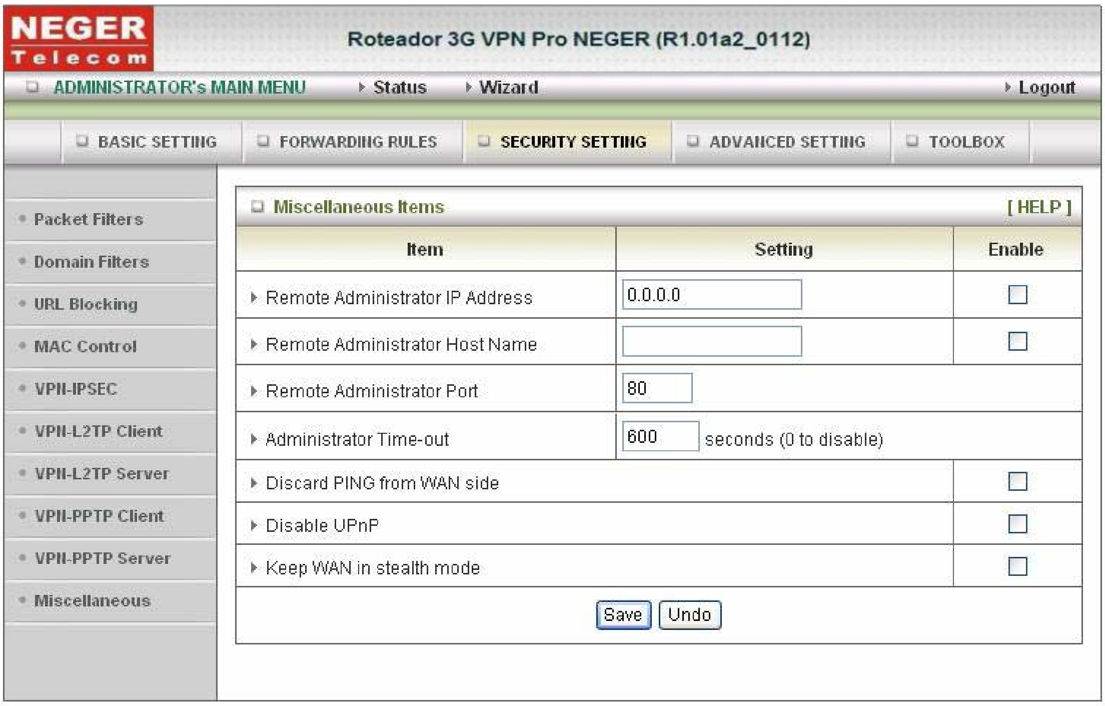
User Account Setting

Users can input five different user accounts for PPTP server.

1. **Tunnel Name:** Input the name for tunnel.
2. **User Name:** Input a user name that is allowed to establish PPTP connection with VPN gateway.
3. **Password**: Input the password for the user.

Click on "Save" to store what you just select or" Undo" to give up

3.2.3.9 Miscellaneous



Miscellaneous Items [HELP]

Item	Setting	Enable
Remote Administrator IP Address	0.0.0.0	□
Remote Administrator Host Name		□
Remote Administrator Port	80	
Administrator Time-out	600 seconds (0 to disable)	
Discard PING from WAN side		□
Disable UPnP		□
Keep WAN in stealth mode		□

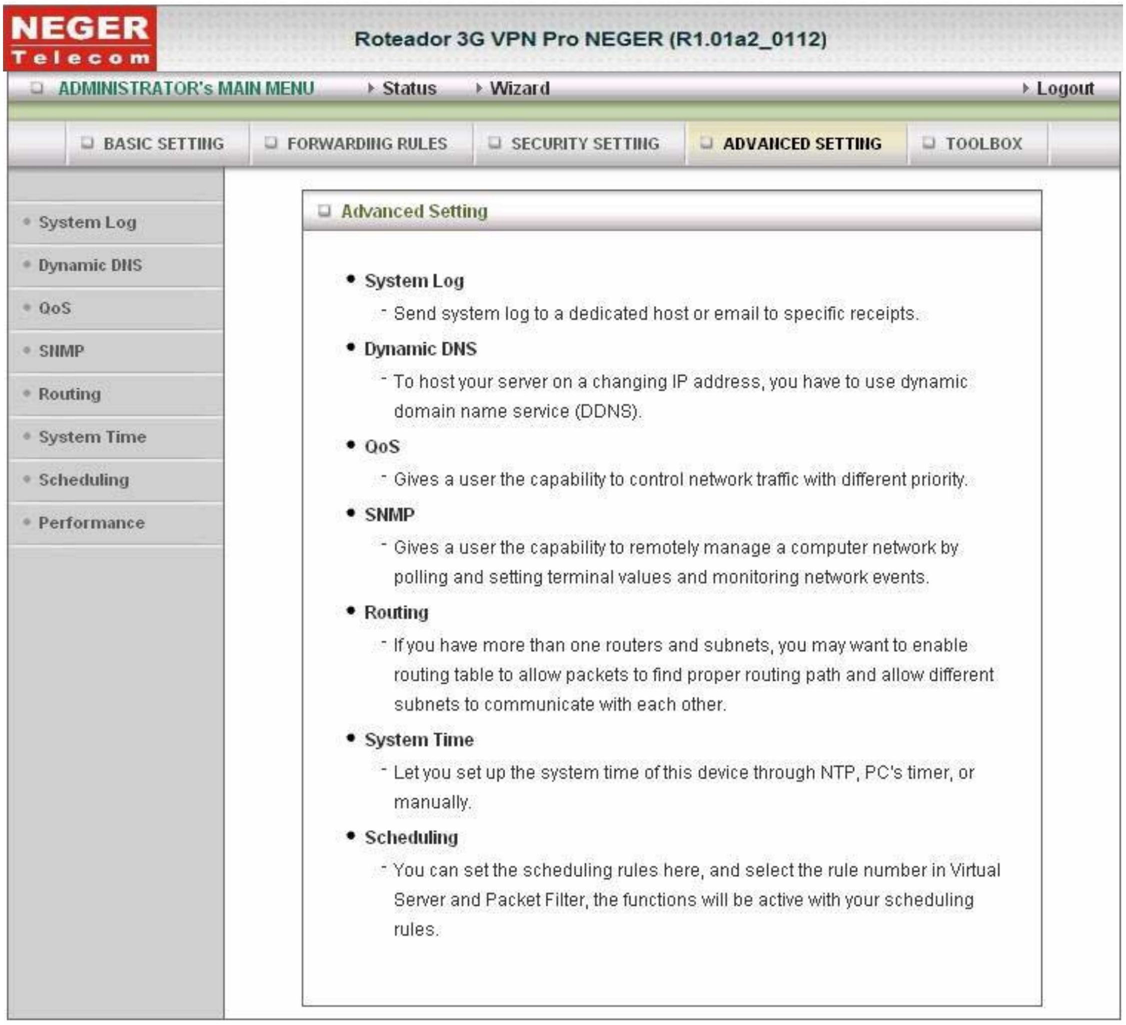
1. **Remote Administrator IP/Host/Port**
   In general, only Intranet user can browse the built-in web pages to perform administration task. This feature enables you to perform administration task from remote host. If this feature is enabled, only the specified IP address can perform remote administration. If the specified IP address is 0.0.0.0, any host can connect to this product to perform administration task. You can use subnet mask bits "/nn" notation to specified a group of trusted IP addresses. For example, "10.1.2.0/24". NOTE: When Remote Administration is enabled, the web server port will be shifted to 88. You can change web server port to other port, too.
2. **Administrator Time-out**
   The time of no activity to logout automatically, you may set it to zero to disable this feature.
3. **Discard PING from WAN side**

   When this feature is enabled, any host on the WAN cannot ping this product.
4. **Disable UPNP**
   The device can disable UPNP function. If your OS supports UPNP search function and you enable UPNP, like Windows XP. You can get Device IP by UPNP.
5. **Keep WAN in stealth mode**

   If the port is not open, the device just to ignore incoming connection attempts, rather than rejecting them.

Click on “Save” to store what you just select or” Undo” to give up

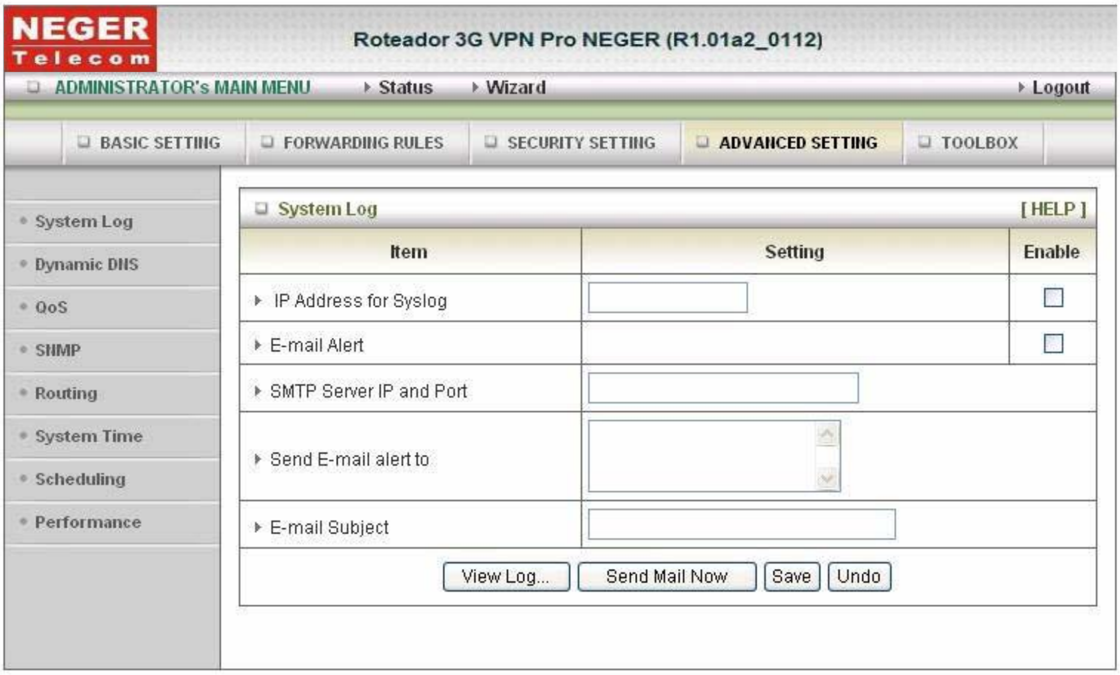
3.2.4 Advanced Setting



Advanced Setting

- System Log
  - Send system log to a dedicated host or email to specific receipts.
- Dynamic DNS
  - To host your server on a changing IP address, you have to use dynamic domain name service (DDNS).
- QoS
  - Gives a user the capability to control network traffic with different priority.
- SNMP
  - Gives a user the capability to remotely manage a computer network by polling and setting terminal values and monitoring network events.
- Routing
  - If you have more than one routers and subnets, you may want to enable routing table to allow packets to find proper routing path and allow different subnets to communicate with each other.
- System Time
  - Let you set up the system time of this device through NTP, PC's timer, or manually.
- Scheduling
  - You can set the scheduling rules here, and select the rule number in Virtual Server and Packet Filter, the functions will be active with your scheduling rules.

3.2.4.1 System Log



Item	Setting	Enable
IP Address for Syslog		□
E-mail Alert		□
SMTP Server IP and Port		
Send E-mail alert to		
E-mail Subject		

This page support two methods to export system logs to specific destination by means of syslog (UDP) and SMTP(TCP). The items you have to setup including:

1. **IP Address for Syslog**

   Host IP of destination where syslog will be sent to.
   Check **Enable** to enable this function.

2. **E-mail Alert Enable**

   Check if you want to enable Email alert (send syslog via email).

3. **SMTP Server IP and Port**

   Input the SMTP server IP and port, which are concatenated with ':'. If you do not specify port number, the default value is 25.
   For example, "mail.your_url.com" or "192.168.1.100:26".

4. **Send E-mail alert to**

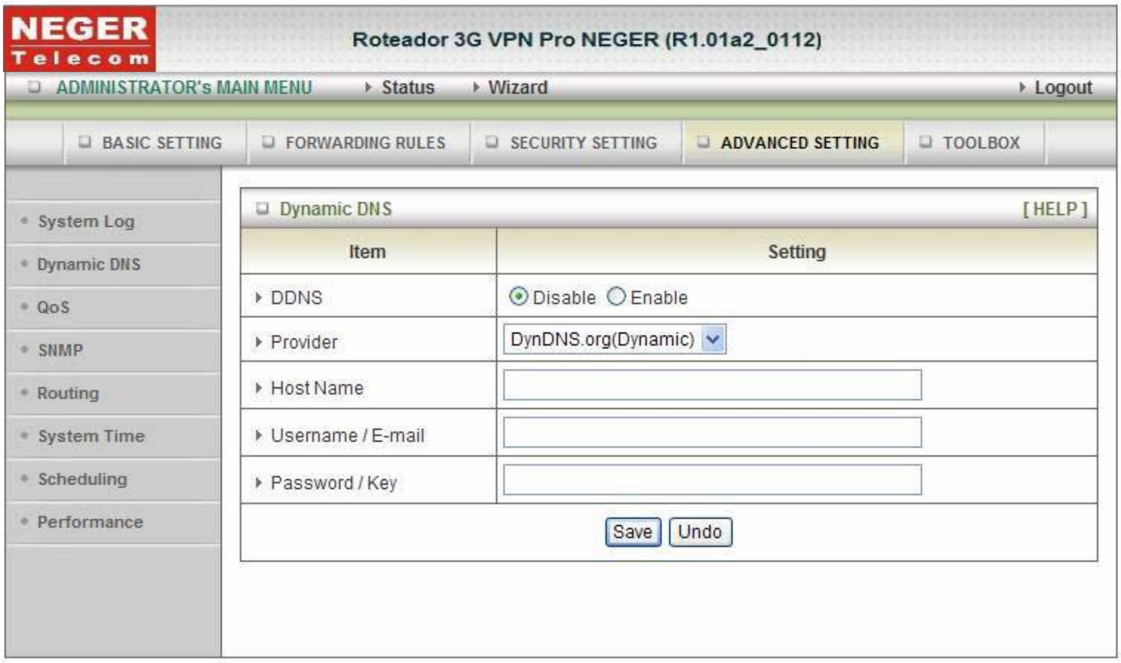
   The recipients who will receive these logs, you can assign more than 1 recipient, using ';' or ',' to separate these email addresses.

5. **E-mail Subject**

   The subject of email alert, this setting is optional.

Click on “Save” to store what you just select or “Undo” to give up

3.2.4.2 Dynamic DNS



Dynamic DNS

Item	Setting
DDNS	● Disable ○ Enable
Provider	DynDNS.org(Dynamic)
Host Name	
Username / E-mail	
Password / Key	

To host your server on a changing IP address, you have to use dynamic domain name service (DDNS).
So that anyone wishing to reach your host only needs to know the name of it. Dynamic DNS will map the name of your host to your current IP address, which changes each time you connect your Internet service provider.

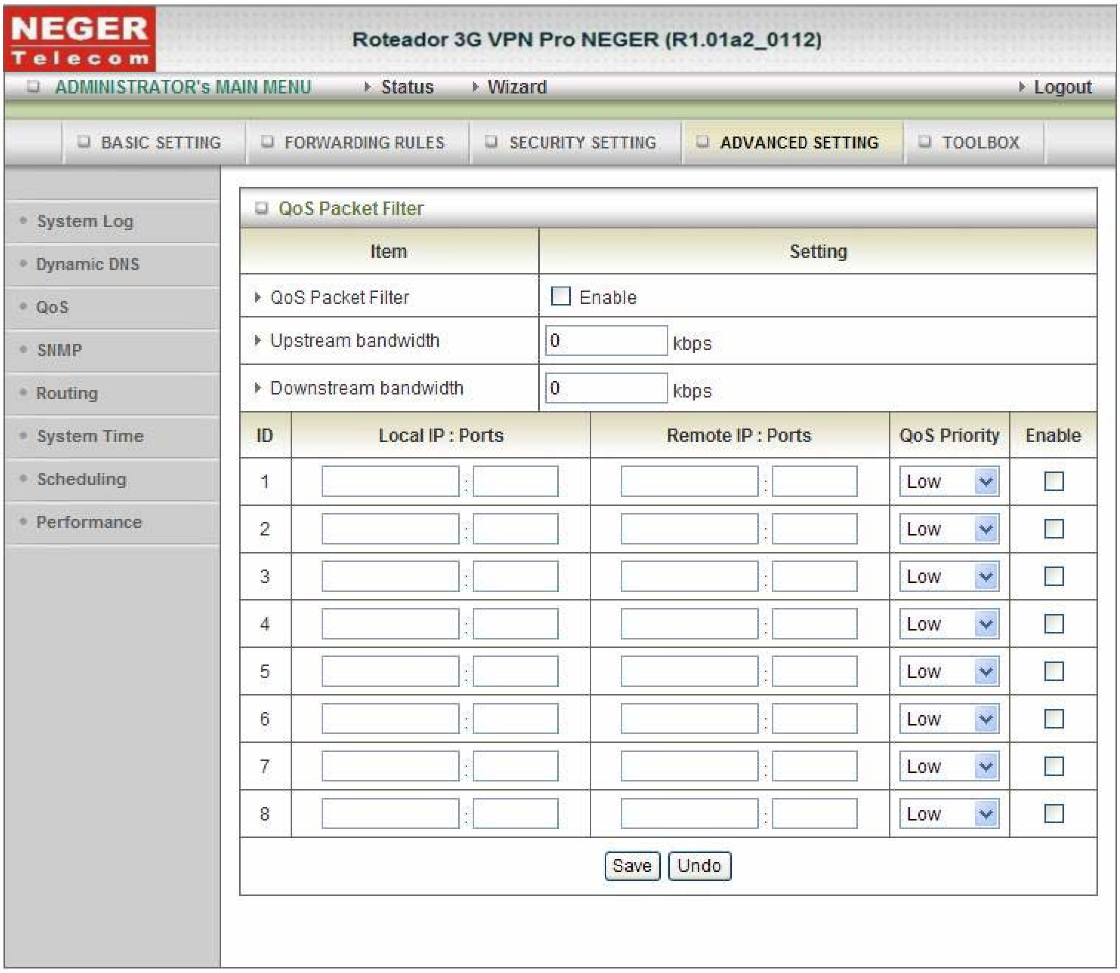
Before you enable Dynamic DNS, you need to register an account on one of these Dynamic DNS servers that we list in provider field.
To enable Dynamic DNS click the check box next to Enable in the DDNS field.
Next you can enter the appropriate information about your Dynamic DNS Server.

You have to define:
Provider
Host Name
Username/E-mail
Password/Key

You will get this information when you register an account on a Dynamic DNS server.

Click on “Save” to store what you just select or “Undo” to give up

3.2.4.3 QOS



QoS Packet Filter

Item	Setting
QoS Packet Filter	□ Enable
Upstream bandwidth	0 kbps
Downstream bandwidth	0 kbps

ID	Local IP : Ports	Remote IP : Ports	QoS Priority	Enable
1	:	:	Low	□
2	:	:	Low	□
3	:	:	Low	□
4	:	:	Low	□
5	:	:	Low	□
6	:	:	Low	□
7	:	:	Low	□
8	:	:	Low	□

Provide different priority to different users or data flows, or guarantee a certain level of performance.

1. **QoS Packet Filter**
   This Item enables QoS function or not.
2. **Upstream Bandwidth**
   Set the limitation of upstream speed.
3. **Downstream Bandwidth**
   Set the limitation of downstream speed.
4. **Local: IP**
   Define the Local IP address of packets here.
5. **Local: Ports**
   Define the Local port of the packets in this field.
6. **Remote: IP**
   Define the Remote IP address of packets here.
7. **Remote: Ports**
   Define the Remote port of the packets in this field.

8. **QoS Priority**

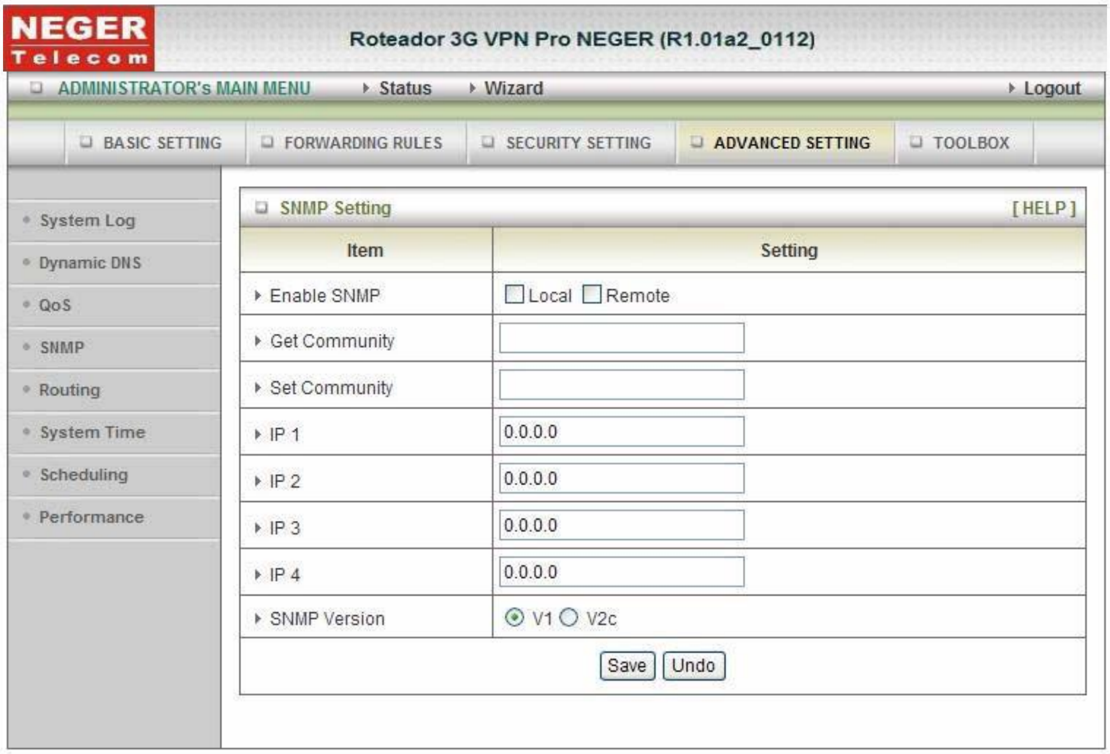
This defines the priority level of the current Policy Configuration. Packets associated with this policy will be serviced based upon the priority level set. For critical applications High or Normal levels are recommended. For non-critical applications select a Low level.

1. **Enable**

Check to enable each rule.

Click on "Save" to store what you just select or "Undo" to give up

3.2.4.4 SNMP



SNMP Setting

Item	Setting
Enable SNMP	□ Local □ Remote
Get Community	
Set Community	
IP 1	0.0.0.0
IP 2	0.0.0.0
IP 3	0.0.0.0
IP 4	0.0.0.0
SNMP Version	● V1 ○ V2c

In brief, SNMP, the Simple Network Management Protocol, is a protocol designed to give a user the capability to remotely manage a computer network by polling and setting terminal values and monitoring network events.

1. **Enable SNMP**

   You must check Local, Remote or both to enable SNMP function. If Local is checked, this device will response request from LAN. If Remote is checked, this device will response request from WAN.

2. **Get Community**

   Setting the community of GetRequest your device will response.

3. **Set Community**

   Setting the community of SetRequest your device will accept.

   IP 1, IP 2, IP 3, IP 4

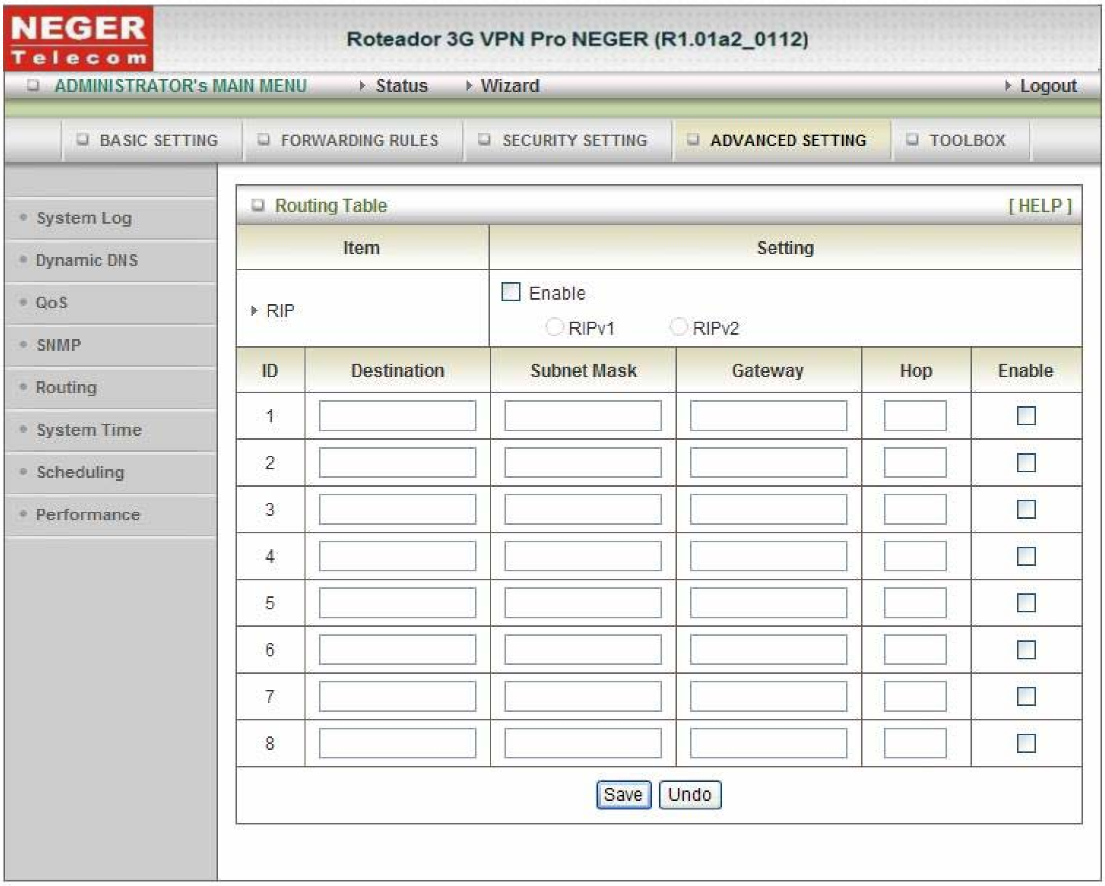
   Input your SNMP Management PC's IP here. User has to configure to where this device should send SNMP Trap message.

4. **SNMP Version**

   Please select proper SNMP Version that your SNMP Management software supports.

Click on "Save" to store what you just select or "Undo" to give up.

3.2.4.5 Routing



Routing Table

Item	Setting
RIP	□ Enable ○ RIPv1 ○ RIPv2

ID	Destination	Subnet Mask	Gateway	Hop	Enable
1					□
2					□
3					□
4					□
5					□
6					□
7					□
8					□

Save Undo

1. **Routing Tables**

   Allow you to determine which physical interface address to use for outgoing IP data grams. If you have more than one routers and subnets, you will need to enable routing table to allow packets to find proper routing path and allow different subnets to communicate with each other.

   Routing Table settings are settings used to setup the functions of static and dynamic routing.

2. **Dynamic Routing**

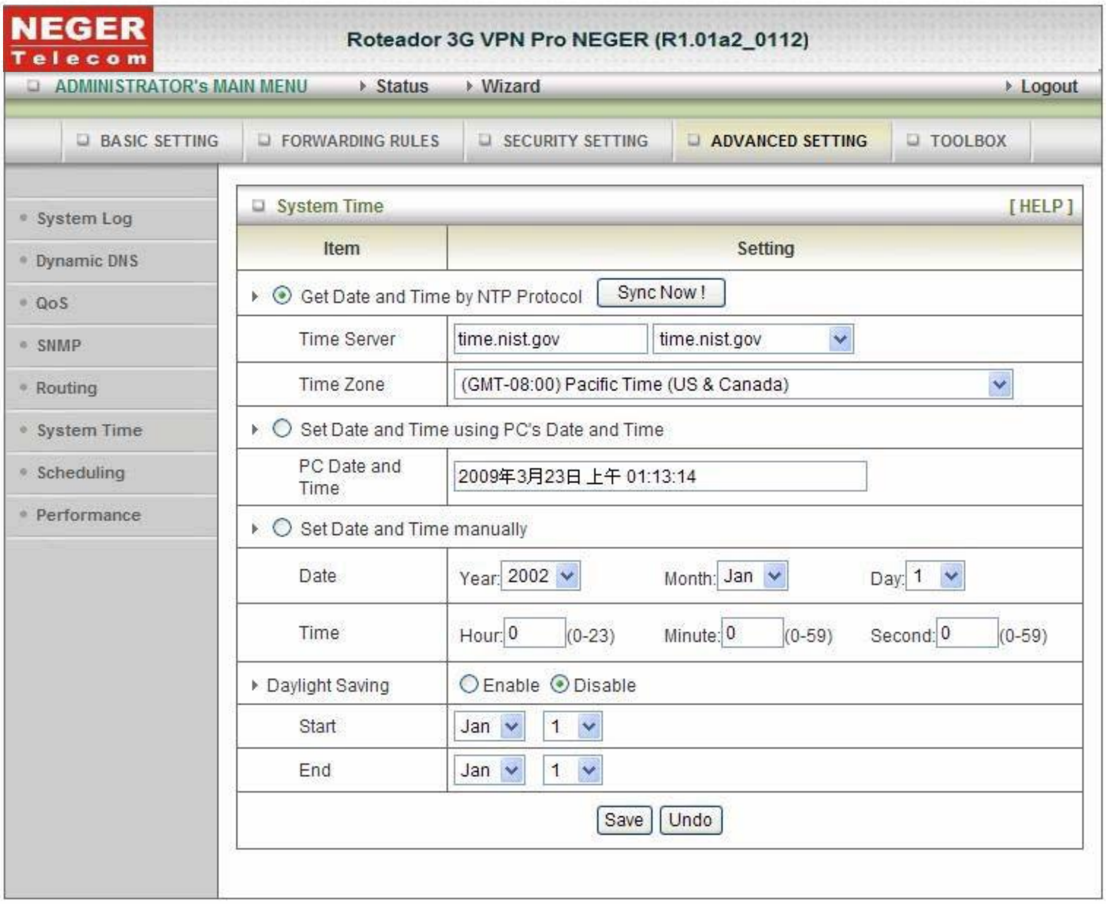
   Routing Information Protocol (RIP) will exchange information about destinations for computing routes throughout the network. Please select RIPv2 only if you have different subnet in your network. Otherwise, please select RIPv1 if you need this protocol.

3. **Static Routing**

   For static routing, you can specify up to 8 routing rules. You can enter the destination IP address, subnet mask, gateway, hop for each routing rule, and then enable or disable the rule by checking or un-checking the Enable checkbox.

Click on "Save" to store what you just select or "Undo" to give up.

3.2.4.6 System Time



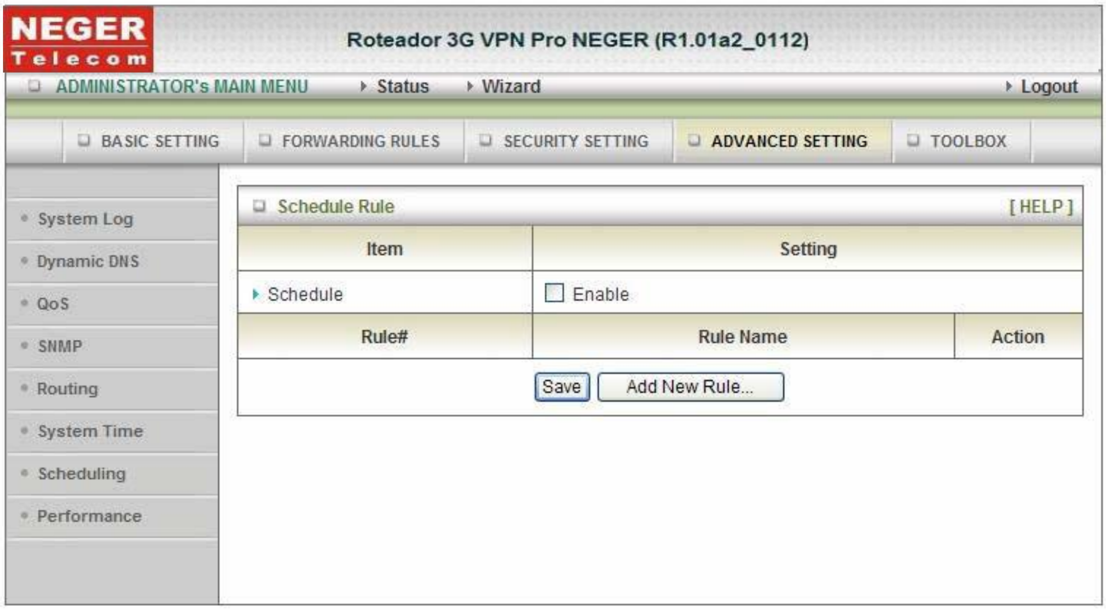
System Time

Item	Setting
● Get Date and Time by NTP Protocol	
Time Server	time.nist.gov · time.nist.gov
Time Zone	(GMT-08:00) Pacific Time (US & Canada)
○ Set Date and Time using PC's Date and Time	
PC Date and Time	2009年3月23日 上午 01:13:14
○ Set Date and Time manually	
Date	Year: 2002 Month: Jan Day: 1
Time	Hour: 0 (0-23) Minute: 0 (0-59) Second: 0 (0-59)
Daylight Saving	○ Enable ● Disable
Start	Jan 1
End	Jan 1

1. **Get Date and Time by NTP Protocol**
   Select if you want to Get Date and Time by NTP Protocol.
   1. **Sync Now:**
      Synchronize system time with network time server
   2. **Time Server**
      Select a NTP time server to consult UTC time
   3. **Time Zone**
      Select a time zone where this device locates.
2. **Set Date and Time manually**
   Select if you want to Set Date and Time manually.
3. **Set Date and Time manually**
   Select if you want to Set Date and Time manually.
4. **Daylight Saving:** Set up the daylight saving period.

Click on "Save" to store what you just select or "Undo" to give up.

3.2.4.7 Scheduling

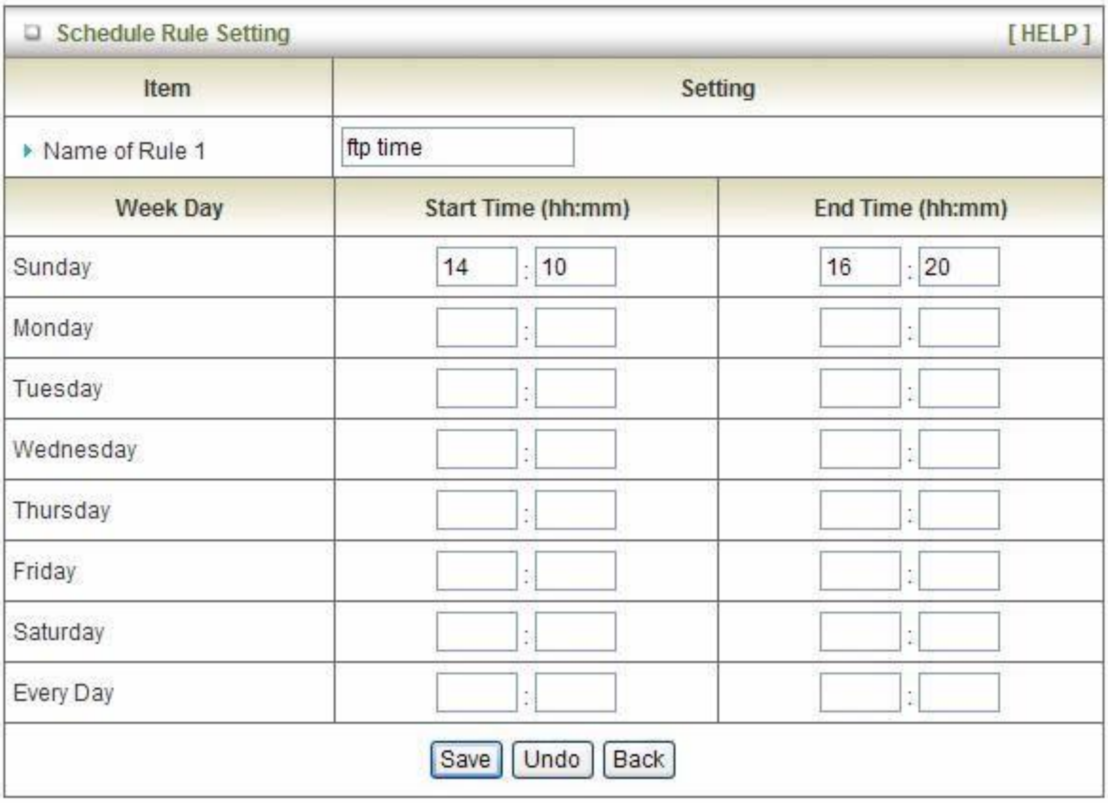


Item	Setting	
Schedule	☐ Enable	
Rule#	Rule Name	Action

You can set the schedule time to decide which service will be turned on or off.
Select the “Enable” item. Press “Add New Rule” You can write a rule name and set which day and what time to schedule from “Start Time” to “End Time”. The following example configure “ftp time” as everyday 14:10 to 16:20

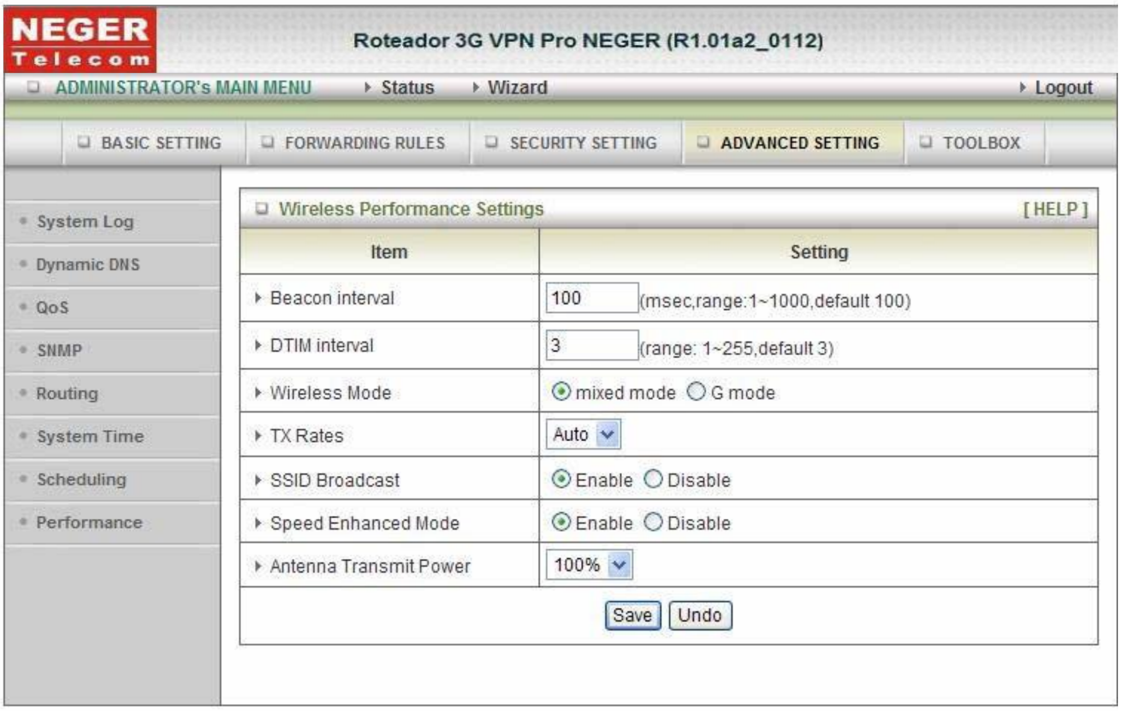
Click on “Save” to store what you just select.

Schedule Rule Setting



Item	Setting	
Name of Rule 1	ftp time	
Week Day	Start Time (hh:mm)	End Time (hh:mm)
Sunday	14 : 10	16 : 20
Monday	:	:
Tuesday	:	:
Wednesday	:	:
Thursday	:	:
Friday	:	:
Saturday	:	:
Every Day	:	:

3.2.4.8 Wireless Performance Settings



Roteador 3G VPN Pro NEGER (R1.01a2_0112)

Wireless Performance Settings

Item	Setting
Beacon interval	100 (msec,range:1~1000,default 100)
DTIM interval	3 (range: 1~255,default 3)
Wireless Mode	● mixed mode ○ G mode
TX Rates	Auto
SSID Broadcast	● Enable ○ Disable
Speed Enhanced Mode	● Enable ○ Disable
Antenna Transmit Power	100%

Save Undo

1. **Beacon Interval**

   Beacons are packets sent by an Access Point to synchronize a wireless network. Specify a Beacon interval value between 1 and 1000. The default value is set to 100 milliseconds.

2. **DTIM interval**：

   Enter a value between 1 and 65535 for the Delivery Traffic Indication Message (DTIM). A DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages. When the Access Point has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. AP clients hear the beacons and awaken to receive the broadcast and multicast messages. The default value for DTIM interval is set to 3

3. **Wireless mode**

   Select wireless connection mode for wireless connection.

4. **TX Rates**

   Select the basic transfer rates based on the speed of wireless adapters on the WLAN (wireless local area network).

5. **SSID Broadcast**

   Choose enable or disable the wireless SSID broadcast. By turning off the broadcast of the SSID ,it is possible to make your wireless network nearly invisible.

6. **Speed Enhanced Mode**

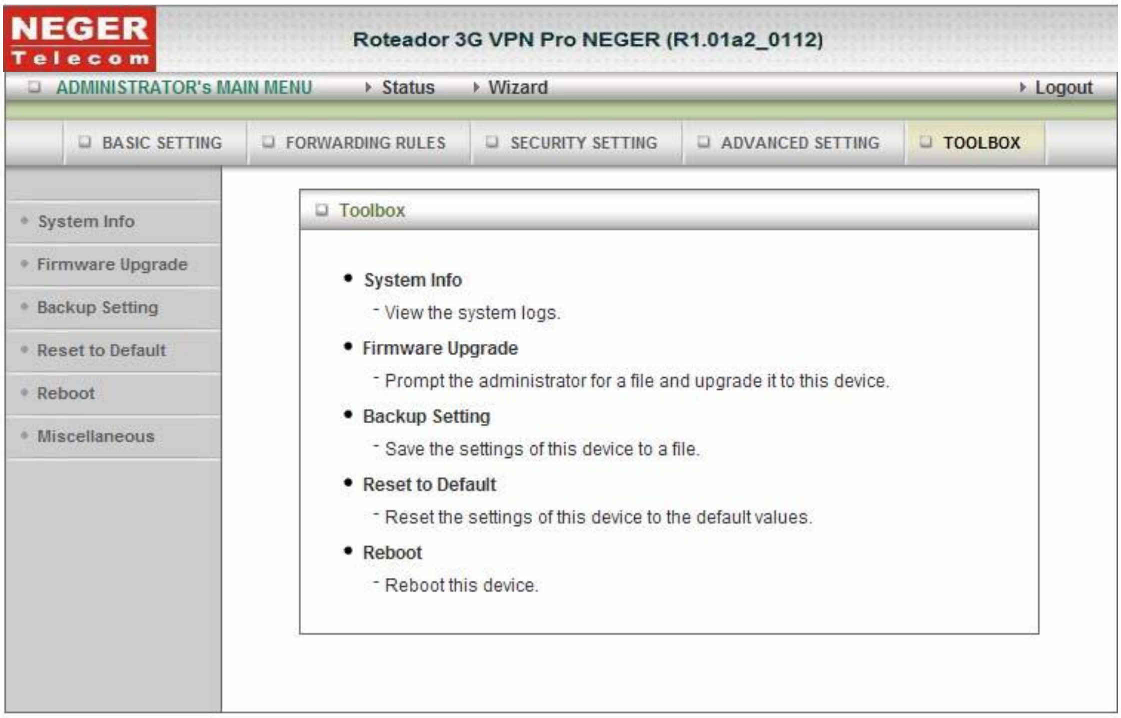
   This is Tx Burst function for Ralink wireless solution

7. **Antenna Transmit Power:**

   Select the Transmit Power of the Antenna.

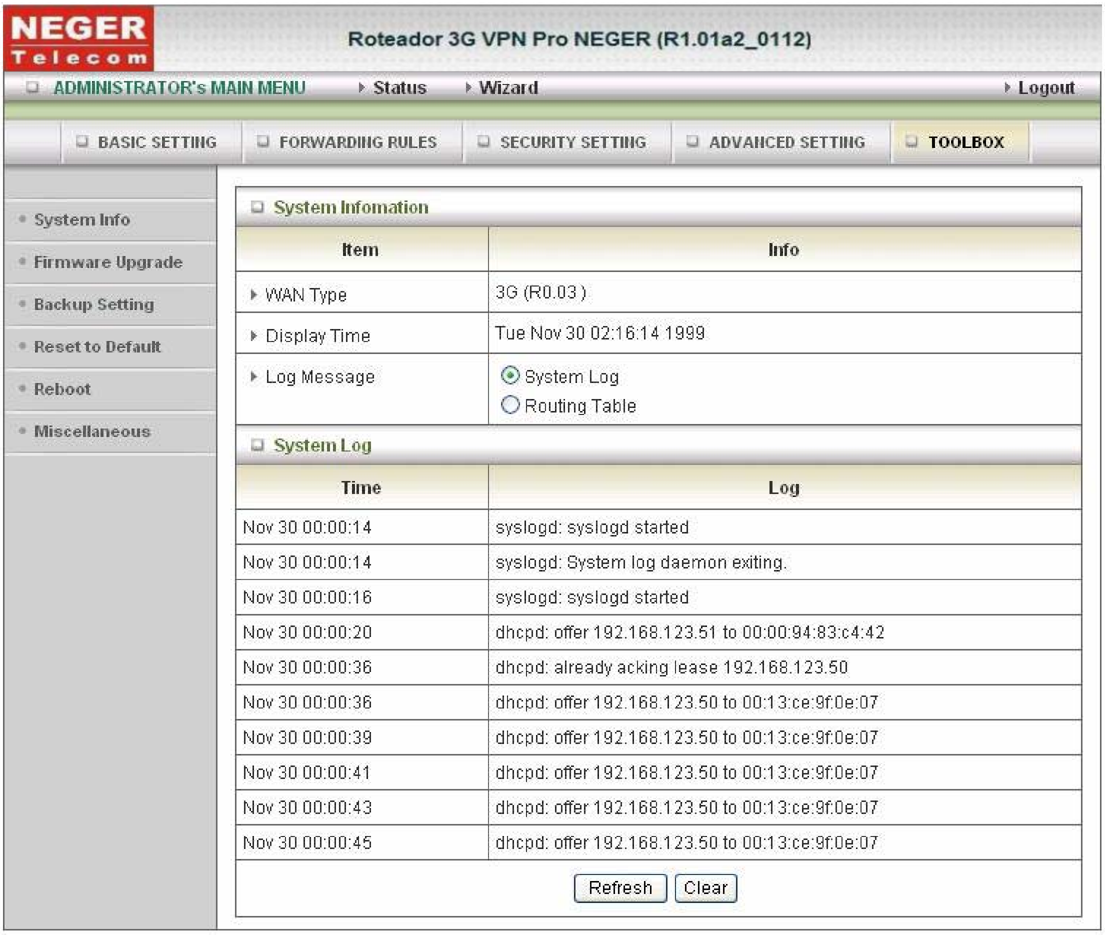
Click on "Save" to store what you just select or "Undo" to give up

3.2.5 Tool Box



- **System Info**
  - View the system logs.
- **Firmware Upgrade**
  - Prompt the administrator for a file and upgrade it to this device.
- **Backup Setting**
  - Save the settings of this device to a file.
- **Reset to Default**
  - Reset the settings of this device to the default values.
- **Reboot**
  - Reboot this device.

3.2.5.1 System Info



System Infomation

Item	Info
WAN Type	3G (R0.03)
Display Time	Tue Nov 30 02:16:14 1999
Log Message	● System Log ○ Routing Table

System Log

Time	Log
Nov 30 00:00:14	syslogd: syslogd started
Nov 30 00:00:14	syslogd: System log daemon exiting.
Nov 30 00:00:16	syslogd: syslogd started
Nov 30 00:00:20	dhcpd: offer 192.168.123.51 to 00:00:94:83:c4:42
Nov 30 00:00:36	dhcpd: already acking lease 192.168.123.50
Nov 30 00:00:36	dhcpd: offer 192.168.123.50 to 00:13:ce:9f:0e:07
Nov 30 00:00:39	dhcpd: offer 192.168.123.50 to 00:13:ce:9f:0e:07
Nov 30 00:00:41	dhcpd: offer 192.168.123.50 to 00:13:ce:9f:0e:07
Nov 30 00:00:43	dhcpd: offer 192.168.123.50 to 00:13:ce:9f:0e:07
Nov 30 00:00:45	dhcpd: offer 192.168.123.50 to 00:13:ce:9f:0e:07

You can view the System Information and System log.
And clear the System log, in this page.

3.2.5.2 Firmware Upgrade

You can upgrade firmware by clicking “Upgrade” button.

3.2.5.3 Backup Setting

You can backup your settings by clicking the “**Backup Setting”** button and save it as a bin file. Once you want to restore these settings, please reference the Section 3.2.5.2 **Firmware Upgrade**.

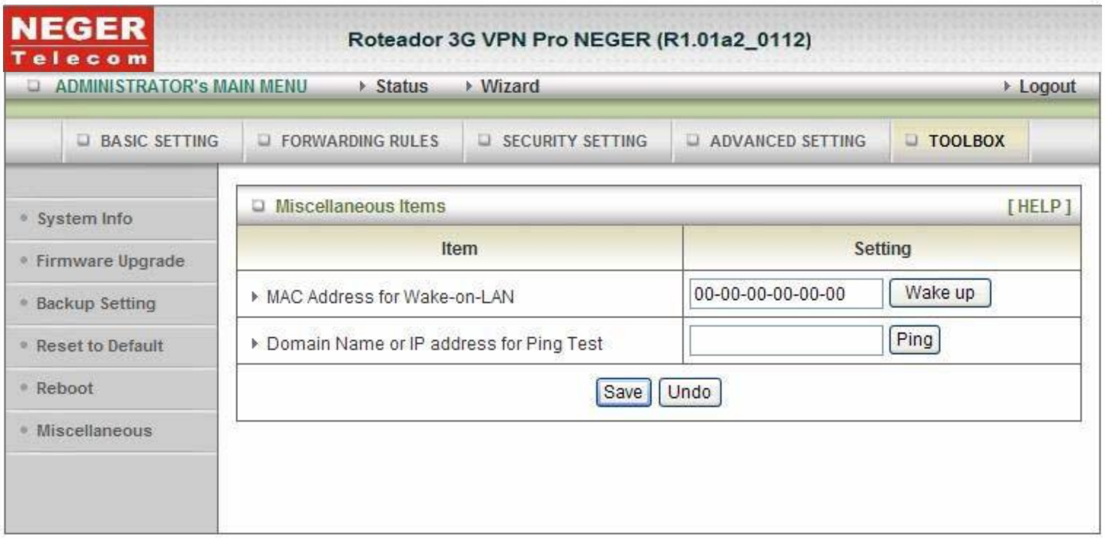
3.2.5.4 Reset to Default

You can also reset this product to factory default by clicking the **Reset to default** button.

3.2.5.5 Reboot

You can also reboot this product by clicking the **Reboot** button.

3.2.5.6 Miscellaneous



Miscellaneous Items [HELP]

Item	Setting
MAC Address for Wake-on-LAN	00-00-00-00-00-00 Wake up
Domain Name or IP address for Ping Test	Ping

1. **MAC Address for Wake-on-LAN**

   Wake-on-LAN is a technology that enables you to power up a networked device remotely. In order to enjoy this feature, the target device must be Wake-on-LAN enabled and you have to know the MAC address of this device, say 00-11-22-33-44-55. Clicking "Wake up" button will make the router to send the wake-up frame to the target device immediately.

2. **Domain Name or IP address for Ping Test**

   You can key in URL or IP address, and then click the “Ping” button for test.

4. Troubleshooting

This section provides an overview of common issues, and possible solutions for the installation and operation of the **NEGER VPN Pro 3G Router**.

1. Unable to access the Configuration Menu when I use my computer to configure the route Why?

Note: It is recommended that you use an Ethernet connection to configure the router

Ensure that the **Ethernet LED** on the **NEGER VPN Pro 3G Router** is **ON**.
If the **LED** is **NOT ON**, check to see if the cable for the Ethernet connection is securely inserted.

> **Note:** Ensure that the **IP Address** is in the same range and subnet as the **NEGER VPN Pro 3G Router**. The IP Address of the **NEGER VPN Pro 3G Router** is 192.168.123.254. All the computers on the network must have a unique IP Address within the same range (e.g., 192.168.123.x). Any computers that have identical IP Addresses will not be visible on the network. All computers must also have the same subnet mask (e.g., 255.255.255.0).

Do a **Ping test** to make sure that the **NEGER VPN Pro 3G Router** is responding.

Go to **Start > Run**.

1:Type **cmd**.
2:Press **Enter.**
3:Type "**ping 192.168.123.254". ** A successful ping shows four replies.

> **Note:** If you have changed the **default** IP Address, ensure you ping the correct IP Address assigned to the **NEGER VPN Pro 3G Router**.

Ensure that your Ethernet Adapter is working properly, and that all network drivers are installed properly.

> **Note:** Network adapter names will vary depending on your specific adapter. The installation steps listed below are applicable for all network adapters.

1. Go to **Start > My Computer > Properties**.
2. **Select** the **Hardware Tab**.
3. Click **Device Manager**.
4. Double-click on "**Network Adapters"**.
5. Right-click on **Wireless Cardbus Adapter**, or **your specific network adapter**.
6. Select **Properties** to ensure that all drivers are installed properly.
7. Look under **Device Status** to see if the device is working properly.
8. Click "**OK"**.

2**: Why my wireless client can NOT access the Internet?**

Note: Establish WiFi Connection. As long as you select either **WEP** or **WPA-PSK** encryption, ensure encryption settings match your WiFi settings. Please refer to your WiFi adapter documentation for additional information.

Ensure that the wireless client is associated and joined with the correct Access Point.
To check this connection, follow the steps below:

1. **Right-click** on the **Local Area Connection icon** in the taskbar.
2. Select **View Available Wireless Networks in Wireless Configure**. The **Connect to Wireless Network** screen appears. Ensure you have selected the correct available network.

Ensure the IP Address assigned to the wireless adapter is within the same subnet as the Access Point and gateway. The **NEGER VPN Pro 3G Router** has an IP Address of **192.168.123.254.** Wireless adapters must have an IP Address in the same range (e.g., 192.168.123.x). Although the subnet mask must be the same for all the computers on the network, no two devices may have the same IP Address. Therefore, each device must have a unique IP Address.

To check the **IP Address** assigned to the wireless adapter, follow the steps below:
1.Enter ipconfig /all in command mode
2.Enter ping 192.168.123.254.to check if you can access the **NEGER VPN Pro 3G Router**.

3. Why does my wireless connection keep dropping?
You may try following steps to solve.

- Antenna Orientation.
  1: Try different antenna orientations for the **NEGER VPN Pro 3G Router**.
  2: Try to keep the antenna at least 6 inches away from the wall or other objects.
- Try changing the channel on the **NEGER VPN Pro 3G Router**, and your Access Point anc Wireless adapter to a different channel to avoid interference.
- Keep your product away (at least 3-6 feet) from electrical devices that generate RF noise, like microwaves, monitors, electric motors, etc.

4. Why I am unable to achieve a wireless connection?
Note: An Ethernet connection is required to troubleshoot the **NEGER VPN Pro 3G Router**
If you have enabled Encryption on the **NEGER VPN Pro 3G Router**, you must also enable encryption on all wireless clients in order to establish a wireless connection.

- For 802.11g, the encryption settings are: 64 or 128 bit. Ensure that the encryption bit level is the same for both the **NEGER VPN Pro 3G Router**, and your Wireless Client.
- Ensure that the SSID (Service Set Identifier) on the **NEGER VPN Pro 3G Router** and the Wireless Client are exactly the same.
  If they are not, your wireless connection will not be established.
- Move the **NEGER VPN Pro 3G Router** and the wireless client into the same room, and then test the wireless connection.
- Disable all security settings such as **WEP**, and **MAC Address Control**.
- Turn off the **NEGER VPN Pro 3G Router** and the client.
  Turn the **NEGER VPN Pro 3G Router** back on again, and then turn on the client.
- Ensure that all devices are set to **Infrastructure** mode.
- Ensure that the LED indicators are indicating normal activity. If not, ensure that the AC power and Ethernet cables are firmly connected.
- Ensure that the IP Address, subnet mask, gateway and DNS settings are correctly entered for the network.
- If you are using 2.4GHz cordless phones, X-10 equipment, or other home security systems, ceiling fans, or lights, your wireless connection may degrade dramatically, or drop altogether.

To avoid interference, change the Channel on the **NEGER VPN Pro 3G Router**, and all devices in your network.

- Keep your product at least 3-6 feet away from electrical devices that generate RF noise. Examples include: microwaves, monitors, electric motors, and so forth.

5. I just do not remember my encryption key. What should I do?

- If you forgot your encryption key, the WiFi card will be unable to establish a proper connection. If an encryption key setting has been set for the **NEGER VPN Pro 3G Router**, it must also be se for the WiFi card that will connect to the **NEGER VPN Pro 3G Router**.
  To reset the encryption key(s), login to the **NEGER VPN Pro 3G Router** using a wired connection. (Please refer to "Basic > Wireless (Security–No Encryption)" on page 10, for additional information).

7. How do I reset my NEGER VPN Pro 3G Router to its factory default settings?
If other troubleshooting methods have failed, you may choose to **Reset** the **NEGER VPN Pro 3G Router** to its factory default settings.
To hard-reset the **NEGER VPN Pro 3G Router** its factory **default** settings, follow the steps listed below:

1. Ensure the **NEGER VPN Pro 3G Router** is powered on
2. Locate the **Reset** button on the back of the **NEGER VPN Pro 3G Router**.
3. Use a paper clip to press the **Reset** button.
4. Hold for 10 seconds and then release.
5. After the **NEGER VPN Pro 3G Router** reboots, it is reset to the factory **default** settings.
   Note: Please note that this process will take a few minutes.

8. What is VPN?

- VPN stands for "Virtual Private Networking." VPNs create a "tunnel" through an existing Internet connection using PPTP (Point-to-Point Tunneling Protocol) or IPSec (IP Security) protocols with various encryption schemes including Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) .
- This feature allows you to use your existing Internet connection to connect to a remote site with added security. If your VPN connection is not functional, verify that your VPN dial-up configuration is correct.
  Note: This information should be provided to you from your VPN provider.
  Pressing the Reset Button restores to its original factory **default** settings.

9. What can I do if my Ethernet cable does not work properly?

- First, ensure that there is a solid cable connection between the Ethernet port on the Router, and your NIC (Network Interface Card).
- Second, ensure that the settings on your NIC adapter are "Enabled," and set to accept an IP address from the DHCP.
- If settings appear to be correct, ensure that you are *not* using a crossover Ethernet cable.

Although the **NEGER VPN Pro 3G Router** is MDI/MDIX compatible, not all NICs are. Therefore, it is recommended that you use a patch cable when possible.

5. Technical Specifications

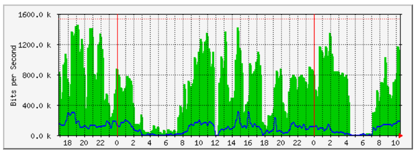
3G Access	USB port
Standards	IEEE 802.11b/g IEEE 802.3 IEEE 802.3u
Wireless	
Standard	IEEE 802.11 B/G

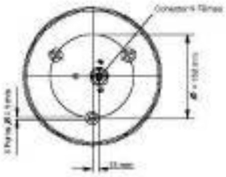
Data Rate	54, 48, 36, 24, 18, 12, 9, and 6 Mbps per channel, Auto Fall-Back
Frequency	2.4 – 2.462 GHz, CCK / OFDM modulation
Range Coverage	Tx/Rx power 18dbm/Per Cell indoors approx. 35-100 meters; outdoors up to 100-300 meters
# of Channels	1-11 for N. America (FCC);1-11 for Canada (DOC) 1-13 Europe (Except Spain and France) (ETSI) 1-14 Japan (TELEC);
Security	64-bit and 128-bit WEP Encryption; WPA encryption
Antenna	Detachable Antenna 1.8dBI
Firewall	IP Filtering NAT (Network Address Translation) with VPN Pass through MAC Filtering
Supported WAN type	3G,Static IP, Dynamic IP, PPPoE,PPTP,L2TP
Connection Scheme	Connect-on-demand, Auto-Disconnect
NAT function	Class C ;One-to-Many; Max 253 Users; Virtual Server; DMZ Host
VPN	PPTP, L2TP and IPSec
Config.& Management	Web-Based IE, Navigator browser and SNMP
	DHCP Server and Client
Working Environment	Temperature: 0~40^{o}C, Humidity 10%~90% non-condensing
OS supported	Windows 95/98/ME/NT/2000/XP; Linux
Power	Switching 12V 2.0A

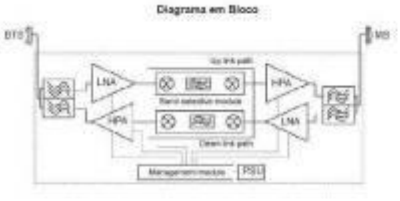
6. Company Profile

NEGER Telecom, based in Campinas, SP - Brazil is an important provider of radio frequency (RF) planning and optimization engineering services to wireless service providers and final users.

Founded in 1987 by engineers and technicians with extensive field experience in telecommunications, NEGER Telecom expertise extends from the conception and development of wireless infrastructure to planning, deployment, and optimization of wireless systems.







NEGER Telecom has rapidly established itself as an innovative company in providing advanced engineering implementations. The company's broad, focused on wireless telecommunications segments – from equipment to *turn key* applications – enables us to efficiently design and implement very efficient solutions. **NEGER Telecom** engineering consulting projects have met with complete success and client satisfaction in many of our implementations in Brazil.

NEGER Telecom has designed wireless systems in main Brazilian cities for telecommunications operators and large companies:

Telefonica (Fixed and Mobile Telecommunication Operator)
More than 2,000 Fixed Cellular Stations planned, projected and installed since 1993. These stations were implemented using 800 MHz AMPS analog technologies (1993-1999) and 800 MHz CDMA digital platforms (1999-2006) in about 200 cities in Brazil (São Paulo state countryside) for a rural fixed telephone service called Ruralcel, including operation and maintenance outsourcing.

British Telecom (Fixed and Mobile Telecommunication Operator)
More than 80 channels of Fixed Cellular Stations installed in sites in São Paulo, Indaiatuba, Vinhedo and Itupeva, integrating a Least Cost Routing Service using 800 MHz digital CDMA technology.
Internet Service Providing in a corporate network in São Paulo State.

Claro (Mobile Telecommunication Operator)
RF repeater plan, project and implementation in Brazilian main cities (São Paulo, Campinas, Santos, São José dos Campos, Ribeirão Preto) for 800 MHz TDMA cellular network and 1800 MHz GSM cellular network. Applications for indoor (airports, shopping malls, corporate customers, etc) and outdoor (delimited areas).
Site survey, system optimization and benchmarking for 800 MHz TDMA and 1800 MHz GSM networks.
Non ionizing antenna radiation study and regulatory consulting for Radio Base Stations installed in Manaus and São José do Rio Preto. Analysis of international standards and RF limits for labor and general population health in order to fulfill all compliances and laws.

TIM (Mobile Telecommunication Operator)
12 channels of Fixed Cellular Stations installed in São Paulo state, integrating a Least Cost Routing Service using 1800 MHz digital GSM technologies.
Non ionizing antenna radiation study and regulatory consulting for Radio Base Stations installed in the Brazilian South Region. Analysis of international standards and RF limits for labor and general population health in order to fulfill all compliances and laws.

Ericsson (Telecommunications Industry and Services)
More than 60 channels of Fixed Cellular Stations installed in São Paulo, Rio de Janeiro, São José dos Campos e Indaiatuba, integrating a Least Cost Routing Service using 800 MHz digital CDMA and 1800 MHz digital GSM technologies.

IBM (IT Services)
More than 60 channels of Fixed Cellular Stations installed in sites in São Paulo, Rio de Janeiro e Hortolândia integrating a Least Cost Routing Service using 800 MHz digital CDMA and 800 MHz TDMA technologies.

GE Mabe (Metallurgic Industry)
12 channels of Fixed Cellular Stations installed in Campinas at Mabe plant, integrating a Least Cost Routing Service using 800 MHz digital CDMA technology.

DHL (Logistic and Courier Services)
More than 20 channels of Fixed Cellular Stations installed in Itupeva at DHL distribution center, integrating a Least Cost Routing Service using 800 MHz digital CDMA and 800 MHz digital TDMA technologies.

Bosch (Mechanical Industry)
More than 40 channels of Fixed Cellular Stations installed in Campinas at two Robert Bosch plants, integrating a Least Cost Routing Service using 800 MHz digital CDMA, 800 MHz digital TDMA and 1800 MHz digital GSM technologies.

Unilever (Consumer Industry)
More than 80 channels of Fixed Cellular Stations installed in sites in São Paulo, Indaiatuba and Vinhedo, integrating a Least Cost Routing Service using 800 MHz digital CDMA technology.

Petrobrás (Oil Industry)
Fixed cellular stations installed in oil processing centers in remote areas of the interior and coast of São Paulo state. Data transmitting and backup communication for the main critical satellite data network using analog AMPS and digital CDMA technologies.

NET (Cable TV Operator)
More than 60 channels of Fixed Cellular Stations installed in sites in Americana, Santo André and Manaus, integrating a Least Cost Routing Service using 800 MHz digital CDMA, 800 MHz digital TDMA and 1800 MHz digital GSM technologies.

Unicamp (State University of Campinas)
More than 30 channels of Fixed Cellular Stations installed in Funcamp administrative center and Hospital area , integrating a Least Cost Routing Service using 800 MHz digital CDMA, 800 MHz digital TDMA and 1800 MHz digital GSM technologies.

Radio Frequency Engineering

Wireless networks never operate well by chance. Careful planning and optimizing are critical to ensure that a wireless network performs as well as possible. The main objective is providing service that has the highest level of station **accessibility** and **call retainabillity**.

The success of the service provider and manufacturer is based on how satisfied the end user is with the level of service that is received. In order to provide an optimum level of service, the wireless network must continue to be improved, requiring an ever-evolving process of implementation, measurement and analysis.

That is the **NEGER Telecom** RF Engineering mission: **Maximize Network Performance at Minimal Cost**.

Our Contacts

Name	Area	Phone	Extension	E-mail
Breno Cicilio	Sales	+55 19 3212 1930	20	breno.cicilio@neger.com.br
Camila Squizani	Sales	+55 19 3212 1930	24	camila.squizani@neger.com.br
Carla Andressa	Sales	+55 19 3212 1930	20	carla.andressa@neger.com.br
Cinara Cardoso	Administrative	+55 19 3237 2121	24	cinara.cardoso@neger.com.br
Cleovis Mendes	Sales	+55 19 3212 1930	20	cleovis.mendes@neger.com.br
Clóvis Cabreira	R&D	+55 19 4141 3455	23	clovis.cabreira@neger.com.br
Daniela Campos	Sales	+55 19 3237 2121	20	daniela.campos@neger.com.br
Danilo Zanini	Engineering	+55 19 3237 2121	28	danilo.zanini@neger.com.br
Diego Sueiro	R&D	+55 19 4141 3454	28	diego.sueiro@neger.com.br
Eduardo Belloti	R&D	+55 19 4141 3454	29	eduardo.belloti@neger.com.br
Eduardo Neger	Engineering	+55 19 3237 2121	31	engenharia@neger.com.br
Eduardo B. Neger	Administrative	+55 19 3254 6275	-	comercial@neger.com.br
Elis Cláudia	Administrative	+55 19 3237 2121	22	elis.claudia@neger.com.br
Elis Cláudia	Administrative	+55 19 4141 3454	30	elis.claudia@neger.com.br
Fábio Lima	Engineering	+55 19 3237 2121	29	fabio.lima@neger.com.br
Henrique Lisboa	Sales	+55 19 3212 1930	20	henrique.lisboa@neger.com.br
Igor Bahamonde	R&D	+55 19 4141 3455	20	igor.bahamonde@neger.com.br
José Netto	Engineering	+55 19 3237 2121	27	jose.netto@neger.com.br
Marco Maraccini	R&D	+55 19 4141 3454	26	marco.maraccini@neger.com.br
Maria Elisa	Administrative	+55 19 3254 6275	-	-
Nelson Junior	Sales	+ 55 19 3212 1930	20	nelson.junior@neger.com.br
Paulo Pinheiro	Engineering	+55 19 3237 2121	28	paulo.pinheiro@neger.com.br
Rodrigo Hodgson	P&D	+ 55 19 4141 3455	22	rodrigo.hodgson@neger.com.br
Rogério Calsavara	P&D	+ 55 19 4141 3455	21	rogerio.calsavara@neger.com.br
Rogério Vale	P&D	+ 55 19 4141 3455	24	rogerio.vale@neger.com.br
Sebastião de Sá	Engineering	+ 55 19 3367 4596	-	sebastiao.sa@neger.com.br
Solange Cavalheri	Administrative	+ 55 19 3212 1930	21	solange.cavalheri@neger.com.br
Thomaz Albrecht	Sales	+ 55 19 3212 1930	20	thomaz.albrecht@neger.com.br
Walter Fernandes	Sales	+55 19 3212 1930	20	walter.fernandes@neger.com.br
Wellington Souza	Engineering	+ 55 19 3243 6767	22	wellington.souza@neger.com.br
Wellington Souza	Engineering	+ 55 19 3237 2121	23	wellington.souza@neger.com.br